Privacy and Data Protection Magazine

REVISTA CIENTÍFICA NA ÁREA JURÍDICA

N.º 02 – 2021
ONLINE

Direção Executiva
Cristina Maria de Gouveia Caldeira
Alexandre Sousa Pinheiro

Universidade Europeia

PRIVACY AND DATA PROTECTION CENTRE

Privacy and Data Protection Magazine

Data: Agosto 2021
Publicações: 3 números anuais

ESTATUTO EDITORIAL

1.º Objeto. A Revista Privacy and Data Protection Magazine é uma publicação científica que tem por objeto a Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

2.º Princípios Deontológicos. Tudo o que, nesta Revista, se venha a publicar, obedecerá rigorosamente à metodologia científica do Direito e à sua praxis quotidiana, sem quaisquer ingredientes políticos ou religiosos. Assim, será sempre no respeito dos princípios deontológicos da imprensa periódica e da ética profissional que se pautará a orientação desta Revista.

3.º Propriedade. É proprietária da Revista a ENSILIS – Educação e Formação, Unipessoal Lda, detentora da Universidade Europeia, com sede na Quinta do Bom Nome, Estrada da Correia, n.º 53, 1500-210.

4.º Edição. A edição da Revista está a cargo da Universidade Europeia.

5.º Objetivo. A Revista visa contribuir para a criação e transmissão do conhecimento científico na área da Proteção de Dados Pessoais; Direitos Fundamentais; Direito de Propriedade Intelectual, Direito do Consumo, Direito da Saúde, Direito Digital e Inteligência Artificial.

6.º Direção Executiva e Editorial. A Revista é dirigida por uma diretora: Cristina Maria de Gouveia Caldeira, que é co-coordenadora do Privacy and Data Protection Centre, email: centro.dataprotection@universidadeeuropeia.pt

7.º Colaborações. A Revista publica em acesso aberto artigos doutrinários e outros estudos, legislação e jurisprudência comentadas e recensões de obras científicas.

8.º Conselho Editorial. Após revisão por pares, a seleção dos trabalhos a publicar é feita por um Conselho Editorial integrados por 6 especialistas de reconhecido mérito.

9.º Periodicidade. A Revista terá periodicidade quadrimestral.

10.º Secções. A Revista compreende quatro secções: (i) Artigos Doutrinários; (ii) Outros Estudos; (iii) Legislação e Jurisprudência Comentadas; (iv) Recensões.

11.º Sistema de Publicação. A Revista com publicação online em três línguas (português, inglês e espanhol), pretende ter um alcance nacional e internacional.

Ficha Técnica

Título
Privacy and Data Protection Magazine

Subtítulo
Revista Científica na Área Jurídica

Número
002

Ano de Publicação
2021

Afiliação
Privacy and Data Protection Centre
Universidade Europeia

Autores
Agostinho Oli Koppe Pereira
Alexandre Sousa Pinheiro
Cleide Calgaro
Cristina Maria de Gouveia Caldeira
Deilton Ribeiro Brasil
Francisco Carvoeiras
Jamile Bergamaschine Mata Diz
Leonor Gaspar Pinto
Márcia Santana Fernandes
Natália Antónia
Núbia Franco de Oliveira
Patrícia P. Carneiro

Prefácio
Alexandre Sousa Pinheiro
Cristina Maria de Gouveia Caldeira

Direção Executiva
Cristina Maria de Gouveia Caldeira

ISSN
2184-920X

Número de Registo
127600

Propriedade
Ensilis - Educação e Formação, Unipessoal, Lda.

Chief Executive Officer
Miguel Carmelo

NIPC/NIF
504 669 788

Editor e Redação
Universidade Europeia
Quinta do Bom Nome, Estrada da Correia, 53,
1500-210, Lisboa

Índice

Prefácio

Após o número inaugural, a Privacy and Data Protection Magazine prossegue o seu compromisso de publicação regular, com um número em que são abordados temas de proteção de dados a par de um estudo sociológico sobre o consumo na sociedade atual.

A par de temas clássicos, o atual número investe no tema da inteligência artificial, quer a através da publicação da proposta de regulamento apresentada pela Comissão Europeia acompanhada de uma introdução enquadradora, quer através da recensão a uma obra que versa sobre o tema.

Dentro do Direito positivo atual a matéria é tratada modestamente nas decisões automatizadas previstas no RGPD. Publica-se um artigo comparativo da legislação europeia e legislação brasileira relativa ao tema.

A inteligência artificial será, em futuros números, objeto de tratamento nesta revista a par de outros com ela conexos.

Dentro de áreas conhecidas da proteção de dados publica-se um artigo sobre gestão documental, recursos humanos e dados pessoais em ambiente organizacional. A matéria tem evidente interesse aplicativo em organizações públicas e privadas.

O papel do Supremo Tribunal Federal do Brasil na defesa do direito fundamental à proteção de dados é igualmente tratado nesta edição.

A doutrina tem-se ocupado da natureza dos dados pessoais especialmente quando a legislação permite que disponham de "curso legal" em relações comerciais. Para debater o tema é publicado um artigo em que se debate a natureza de "coisa", sem perda de relação com a dignidade humana, dos dados pessoais.

Em sede de "outros estudos" inclui-se um tema de interesse e atualidade permanentes sobre a proteção de dados de jogadores online. O autor, licenciado em engenharia, apresenta uma visão técnica e funcional da matéria e dos fundamentos legais competentes.

No futuro, constitui intenção da revista publicar mais artigos de áreas técnicas que enriqueçam a abordagem jurídica dos assuntos usualmente tratados.

Por último, são feitas duas recensões críticas, não apologeticas, como tem sido comum, sobre a obra de Carissa Vélez, *Privacy is Power* e sobre *Direito e Inteligência Artificial – em Defesa do Humano*, uma obra de Juarez Freitas e de Thomas Bellini Freitas.

I_Artigos Doutrinários

Recursos humanos, processos e dados pessoais: contributos da Gestão de Informação para a melhoria organizacional

Leonor Gaspar Pinto[1]
Natália Antónia[2]

RESUMO

Esta comunicação visa apresentar a experiência de colaboração intraorganizacional entre duas unidades orgânicas da Câmara Municipal de Lisboa pertencentes a duas áreas funcionais distintas, mas transversais a toda a organização - a Direção Municipal de Recursos Humanos e a Direção Municipal de Cultura, através da sua Divisão de Arquivo Municipal, desenvolvida entre julho de 2018 e setembro de 2019. Esta colaboração teve como principal impulso a abordagem por processos e a implementação, em 2018, no Município de Lisboa do Regulamento Geral de Proteção de Dados (RGPD), equacionadas num contexto mais vasto de Gestão de Informação.
Queremos nesta comunicação, através da partilha de um estudo de caso, demonstrar como o trabalho colaborativo entre duas unidades orgânicas distintas, mas transversais à organização, na área da gestão de informação, como em qualquer outra, se pode transformar numa potente ferramenta para atingir, de forma mais eficiente, objetivos comuns e, ao mesmo tempo, facilitar a aquisição de novos conhecimentos[3].

PALAVRAS-CHAVE

Recursos humanos, Proteção de Dados Pessoais, Gestão de Informação, Gestão por Processos, Avaliação de Documentos

[1] Doutorada em Documentação (Universidad de Alcalá), MSc. in Information Management (University of Sheffield) e licenciada em História (NOVA FCSH). Professora convidada no Mestrado em Gestão e Curadoria da Informação da NOVA FCSH. Investigadora Integrada do CHAM – Centro de Humanidades (NOVA FCSH e Universidade dos Açores). Técnica Superior da Câmara Municipal de Lisboa, é atualmente Coordenadora da Equipa de Projeto de Proteção de Dados Pessoais deste Município.

[2] Licenciada em História pela Faculdade de História da Universidade Estatal de Voronej, URSS e Ph.D. em História pelo Instituto de História Universal da Academia das Ciências da URSS. É especializada em Ciências Documentais – variante de Arquivo, pela Faculdade de Letras da Universidade de Lisboas e Máster en Archivística pela Universidade Carlos III de Madrid. Desde 1993 é Técnica Superior na Câmara Municipal de Lisboa, exercendo, desde 1999, funções no Arquivo Municipal de Lisboa, onde tem desenvolvido funções na área de gestão de documentos, com destaque para a classificação e avaliação da informação pública.

[3] O presente texto foi apresentado no 13.º Encontro Nacional de Arquivos Municipais, que decorreu de 18 a 19 outubro de 2019, em Cascais, tido sido publicado nas respetivas Atas.

Human resources, processes and personal data: Information Management contributions to organizational improvement

ABSTRACT

This paper aims to discusses the intra-organizational collaboration between two organizational units of Lisbon Municipality – the Municipal Directorate of Human Resources and the Municipal Directorate of Culture, through its Division of Municipal Archive -, developed between July 2018 and September 2019. In spite of belonging to different functional areas, both organizational units have cross functions throughout the entire organization.

This collaboration received its main thrust from a process management approach combined with the implementation of the General Data Protection Regulation (GDPR) in Lisbon Municipality, in 2018, both framed by an Information Management perspective.

This case study shows that collaboration between two distinct cross organizational units based on a common information management approach can be a powerful tool to achieve, more efficiently, common goals and, at the same time, facilitate the acquisition of new knowledge.

Keywords: Human Resources, Personal Data Protection, Information Management, Process Management, Document Evaluation.

Introdução

Os últimos anos têm sido marcados por grandes desafios decorrentes de estratégias governativas que visam a modernização administrativa e a transformação digital de toda a Administração Pública, tanto Central, como Local. Em 2016, surge um novo desafio: o *Regulamento n.º 2016/679 do Parlamento Europeu e do Conselho*, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, sobejamente conhecido por todos como Regulamento Geral de Proteção de Dados (RGPD)[4]. Sendo obrigatória desde maio de 2018, o balanço que é feito da implementação do RGPD, decorrido um ano, indica genericamente que ainda há um longo caminho a percorrer nas práticas e na cultura das organizações portuguesas em matéria de proteção de dados pessoais (REIS e FERREIRA, 2019), apesar de se registarem melhorias significativas na sua adaptação a este regulamento. Clara Guerra, da Comissão Nacional de Proteção de Dados (CNPD - a entidade portuguesa que fiscaliza a aplicação do RGPD) prefere salientar que «Foi essencialmente um ano de aprendizagem para todos - para as empresas, as entidades públicas, os cidadãos e, por último, também a CNPD, que teve de lidar com algumas questões novas» (FREIRE, 2019).

Foi com este contexto de adequação e desafio que a Câmara Municipal de Lisboa (CML) aprovou, em reunião de 24 de maio de 2018, a criação da Equipa de Projeto para a Implementação do Regulamento Geral de Proteção de Dados no Município de Lisboa (EPIRGPD) (DELIBERAÇÃO N.º 288/CM/2018). Tendo em conta que uma das competências desta equipa é a «definição de uma estratégia de gestão da informação em conformidade [com o RGPD], incluindo mecanismos de governação de dados e a respectiva arquitectura tecnológica que possibilita a sua implementação» (Deliberação n.º 288/CM/2018, p. 242) percebeu-se de imediato a necessidade de articulação dos diferentes intervenientes no processo. A definição desta estratégia encontra-se largamente condicionada pelas características estruturais específicas da CML, nomeadamente o facto de esta ser o órgão executivo da maior autarquia do país, da sua estrutura orgânica ser composta por 15 direções municipais, 46 departamentos e 100 divisões e de contar atualmente com 170 dirigentes e 7.897 trabalhadores/as[5].

[4] A transposição do RGPD para a ordem jurídica portuguesa só se tornaria efetiva com a publicação, em 2019-08-08, da Lei 58/2019 (*Diário da República* n.º 151/2019, Série I. Disponível em https://dre.pt/home/-/dre/123815982/details/maximized).

[5] Dados referentes a agosto de 2019 (fonte: Divisão de Planeamento e Gestão de Recursos Humanos/ Departamento de Gestão de Recursos Humanos / DMRH).

Assim, a Direção Municipal de Recursos Humanos (DMRH) e a Direção Municipal de Cultura, através da sua Divisão de Arquivo Municipal (DAM), alinharam as suas sinergias e conhecimentos para enfrentar, de forma harmonizada, todos estes desafios, sempre em sintonia com a Equipa de Projeto para a implementação do RGPD.
Tendo por base o acima exposto, a nossa comunicação visa apresentar a experiência de colaboração intraorganizacional desenvolvida entre julho de 2018 e setembro de 2019, por estas duas unidades orgânicas da CML pertencentes a áreas funcionais distintas, mas transversais a toda a organização - a DMRH e a DAM -, equacionada segundo uma perspetiva de Gestão de Informação.

1. Caminhos confluentes

A DMRH é o serviço responsável na CML pela gestão das pessoas que nela trabalham. A sua atuação enquadra-se e decorre do conjunto de competências e atribuições que formalmente lhe estão atribuídas nos termos das estruturas nuclear e flexível dos serviços do Município de Lisboa, aprovadas em 7 de junho de 2018, por deliberação da Assembleia Municipal (DELIBERAÇÃO N.º 305/AML/2018). A sua missão é «Desenvolver e coordenar a implementação de estratégias e práticas de gestão de pessoas, assentes no serviço ao cliente, numa perspetiva de partilha de recursos e de parceria com os serviços, a fim de otimizar o desempenho individual e organizacional» (DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS, 2019, P. 10).

Desde 2012 que a DMRH utiliza como ferramenta de gestão e melhoria contínua a abordagem por processos. A abordagem por processos:

- é uma metodologia de gestão;
- a sua aplicação é um dos requisitos essenciais (0.3) à certificação de um sistema de gestão da qualidade, conforme disposto na NP EN ISO 9001 (2015);
- segue o modelo PDCA (para produtos e serviços), incorporando o contexto da organização e partes interessadas relevantes;
- envolve a definição e a gestão sistemáticas dos processos e das suas interações, de forma a obter os resultados pretendidos de acordo com a política da qualidade e a orientação estratégica da organização.

Na sequência de uma avaliação realizada em 2017, o Projeto Gestão por Processos foi (re)lançado em 2018, com o objetivo de "reajustar o modelo de Gestão por Processos implementado na DMRH, com vista à focalização estratégica do seu desempenho nas

necessidades e expectativas dos/as clientes e, simultaneamente, à obtenção de ganhos de eficiência e eficácia ao nível do seu funcionamento, respondendo às exigências e desafios da Sociedade em Rede" (DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS, 2019, p. 5). Um dos impulsos para esse reajustamento proveio exatamente da necessidade de adequação dos processos geridos pela DMRH ao RGPD, o que ficou claramente refletido na inclusão no Objetivo Operacional 4 («Adotar medidas de normalização, simplificação e desmaterialização de processos») do QUAR - Quadro de Avaliação e Responsabilização para 2018 do indicador «N.º processos otimizados de acordo com o Regulamento Geral de Proteção de Dados (RGPD)» (DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS, 2018).

Paralelamente a este percurso, o início da implementação do RGPD no Município de Lisboa, em maio desse ano, ao sinalizar a área de Recursos Humanos como uma das áreas prioritárias de intervenção, veio gerar uma nova dinâmica de inter-relacionamentos entre unidades orgânicas diferentes, mas partilhando o objetivo de melhorar o tratamento dos dados pessoais dos trabalhadores e trabalhadoras, promovendo a aplicação de boas práticas de gestão da informação. Quando, em resposta à orientação da EPIRGPD para que os serviços da CML procedessem ao registo das operações de tratamento de dados pessoais na AMRAT - Aplicação Municipal de Registo das Atividades de Tratamento, a DMRH utilizou como base de trabalho o seu Catálogo de Processos, tornou-se claro que o apoio da DAM seria importante para a (re)definição dos prazos de conservação dos dados pessoais a cargo da DMRH, armazenados em papel, mas também em formato eletrónico.

A DAM, no âmbito das suas atribuições na «promoção de boas práticas de gestão documental integrada» no Município de Lisboa (DELIBERAÇÃO N.º 305/AML/2018, p. 205), tem participado em diversos projetos de informatização dos serviços, sobretudo de implementação de soluções de "gestão documental", tendo contribuído para a definição dos necessários requisitos de gestão de documentos. As equipas da DAM que têm acompanhado estes projetos defenderam, desde sempre, a necessidade destas soluções abrangerem todo o ciclo de vida dos documentos, desde a sua produção e captura/registo nos sistemas, nomeadamente a sua classificação e avaliação, permitindo de forma automática a determinação dos prazos de conservação administrativa dos documentos, a transferência para repositório secundário dos documentos de conservação permanente e a eliminação daqueles cujos prazos legais de conservação já prescreveram.

Tendo em conta as fragilidades da atual solução de "gestão documental" e a consequente acumulação exponencial de documentação não classificada de acordo com as normas internacionais, a DAM, desde 2005, tem vindo a responder de forma organizada, a solicitações das unidades orgânicas para a transferência para o Arquivo Municipal de documentos que já não são de consulta frequente, procedendo no terreno à sua avaliação, aplicando o Regulamento Arquivístico para as Autarquias Locais, publicado pela Portaria n.º 412/2001, de 17 de abril, alterada pela Portaria n.º 1253/2009, de 14 de outubro. Estas portarias regulamentam a avaliação, seleção e eliminação dos documentos das autarquias locais, bem como os procedimentos administrativos que lhes estão associados. Nesse sentido, a sua aplicação no contexto do Município de Lisboa contribuiu para a normalização dos procedimentos de eliminação de documentos de forma controlada e permitiu, também, que a avaliação de documentos começasse a ser realizada em articulação com os serviços "donos do negócio", ou seja, com os serviços produtores, conduzindo a que só sejam transferidos, para os depósitos do Arquivo, os documentos considerados de conservação definitiva.

Por outro lado, de outubro de 2011 a 2019, a DAM participou, com outras entidades da Administração Local e Central, nos projetos colaborativos promovidos pela Direção-Geral do Livro, dos Arquivos e das Bibliotecas (DGLAB), tendo por objetivo a identificação e a caracterização dos processos de negócio assegurados pelas entidades da Administração Pública, bem como a sua classificação e avaliação. Os produtos desenvolvidos por esta equipa de trabalho tiveram presentes as orientações para a interoperabilidade semântica, decorrentes da *Decisão (UE) 2015/2240 do Parlamento Europeu e do Conselho*, de 25 de novembro de 2015. Do esforço coletivo então desenvolvido, resultou a Lista Consolidada para a classificação e avaliação da informação pública (LC). A LC é uma estrutura hierárquica de classes que representam as funções, subfunções e processos de negócio executados pela Administração Pública, contemplando a sua codificação, a identificação, a descrição e as decisões de avaliação, bem como as respetivas justificações dos Prazos de Conservação Administrativa (PCA) e Destinos Finais (DF) (DIREÇÃO-GERAL DO LIVRO, DOS ARQUIVOS E DAS BIBLIOTECAS, 2019). A Lista Consolidada é o referencial de base para o desenvolvimento de instrumentos organizacionais ou pluriorganizacionais para a classificação e avaliação da informação pública (Plano de Classificação e Tabela de Seleção).

Tendo em conta que as Portarias de Gestão de Documentos para as Autarquias Locais, acima referidas, já se encontram bastante desatualizadas e não permitem uma abordagem por processos, o Grupo de Trabalho que representa as autarquias locais, sob coordenação da DGLAB, preparou uma proposta, para submeter à apreciação do Secretário de Estado das Autarquias Locais. Recentemente, a Associação Nacional de Municípios Portugueses (ANMP) solicitou aos Municípios seus associados, o parecer sobre o projeto de Portaria de Gestão de Documentos para as Autarquias Locais.

A existência de uma determinação legal para a uniformização dos prazos de conservação administrativa, bem como dos destinos finais dos processos de negócio e da sua justificação com base no princípio da finalidade e no fundamento jurídico, traduz-se num elemento crucial e facilitador para a implementação do RGPD que poderia, assim, contribuir para a melhoria da eficiência na gestão de documentos no Município de Lisboa.

2. Aspetos metodológicos

Tendo a Gestão de Informação o enquadramento teórico genérico, procurámos responder à questão de investigação: *Como pode a Gestão de Informação ser utilizada em iniciativas de melhoria intraorganizacional?* por via de uma abordagem qualitativa. Nesse sentido, pretendia-se estudar a experiência de colaboração intraorganizacional (em curso) entre duas unidades orgânicas da CML pertencentes a áreas funcionais distintas, mas transversais a toda a organização - a DMRH e a DAM, pelo que se recorreu à combinação de dois métodos: o estudo de caso, que, de acordo com Yin (2001), é um estudo que investiga um fenómeno contemporâneo em profundidade e dentro do seu contexto real; e a investigação-ação, entendida como uma abordagem que pressupõe que os contextos sociais estão em permanente mudança e que o/a investigador/a e a pesquisa propriamente dita são parte dessa mudança (COLLIS e HUSSEY, 2005).

No âmbito do Projeto Gestão por Processos, os objetivos e plano de ação estabelecidos para o segundo semestre de 2018 e para 2019 foram ajustados de forma a integrarem o planeamento do trabalho colaborativo entre a DMRH e a DAM, com o apoio da EPIRGPD, focalizando-o em três eixos de intervenção prioritária:

Eixo 1 – Redefinição da arquitetura de macroprocessos do negócio da DMRH e mapeamento dos processos.

Eixo 2 - Documentação e otimização do "Processo individual" do trabalhador/a.

Eixo 3 - Documentação e otimização do "Processo de controlo de assiduidade" do trabalhador/a.

O trabalho colaborativo desenvolveu-se essencialmente no quadro das sessões de trabalho da Equipa de Projeto, complementadas por visitas ao terreno e reuniões parcelares específicas. Enquanto membros desta Equipa e responsáveis pela operacionalização da parceria entre a DMRH e a DAM, as investigadoras asseguraram a recolha, análise e organização dos conteúdos gerados coletivamente e, sobretudo, procuram sempre enquadrar as questões suscitadas pela aplicação da abordagem por processos e do RGPD numa perspetiva de Gestão de Informação. Não entrando na discussão em torno do próprio conceito e da sua delimitação epistemológica, consideramos aqui, na linha de T. W. Wilson (2002), que a Gestão de Informação é a aplicação de princípios de gestão para aquisição, organização, controle, disseminação e uso de informação relevante para o funcionamento eficaz de qualquer tipo de organização.

Na análise dos eixos de intervenção foi determinante a mobilização do conceito *ciclo de vida dos documentos*, o qual, numa aceção mais ampla, sustenta o conceito de *ciclo de vida da informação*[6]. Ao período compreendido entre a produção de um documento – incluindo o seu desenho e criação – e a sua eliminação ou conservação permanente, convencionou-se chamar *ciclo de vida dos documentos*. Importa, deste modo, reconhecer que o ciclo de vida não encerra com a conclusão do procedimento administrativo legalmente previsto para cada processo associado a uma área de negócio (ex.: urbanismo, recursos humanos, saneamento, recursos financeiros, etc…), mas apenas após o cumprimento do respetivo prazo de conservação administrativa, através da sua eliminação ou conservação, sendo esses prazos e destinos também fixados legalmente.

O RGPD incorpora esta ideia de "ciclo" quando, ao definir «tratamento [de dados pessoais]», lista as respetivas operações do seguinte modo: «a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição» (artigo 4.º, n.º 2, do RGPD). A integração na abordagem por processos desta perspetiva, reforçada pela necessidade de adequação aos requisitos do RGPD, obrigaria a DMRH a dar especial atenção às etapas de criação e de eliminação ou conservação dos dados/documentos, bem como à respetiva tipologia dos suportes, aquando da revisão dos seus processos de negócio.

[6] «The idea of an information life cycle is derived from records management, where the idea of document life cycle is central to the overall process» (Wilson, 2002, p. 266).

3. Análise e discussão dos resultados

Tratando-se de uma experiência de colaboração intraorganizacional que assenta numa dinâmica de envolvimento e participação dos/as vários/as intervenientes e que se encontra ainda a decorrer, muitos dos resultados apurados são ainda preliminares ou não alcançaram ainda a etapa final prevista para a sua realização. Importa ter presente que, entre junho de 2018 e setembro de 2019, para além de outras reuniões específicas e visitas ao terreno, o Projeto Gestão por Processos já realizou 21 sessões de trabalho, em que estiveram presentes os membros da Equipa de Projeto e, em 14 delas, técnicos/as da DAM, mas também os/as Dirigentes da DMRH, a Chefe de Divisão da DAM e, numa dessas sessões, o Encarregado de Proteção de Dados da CML.

Eixo 1 – Redefinição da arquitetura de macroprocessos do negócio da DMRH e mapeamento dos processos

A reflexão e compreensão das semelhanças e diferenças entre os conceitos-chave utilizados pela DMRH e pela DAM no âmbito da Gestão por Processos constituíram uma etapa importante, uma vez que permitiu o entender dos conceitos subjacentes aos trabalhos já realizados pelas duas unidades orgânicas e encontrar uma linguagem comum.

O Quadro 1 apresenta o(s) significado(s) atribuído(s) aos principais conceitos mobilizados no contexto do trabalho colaborativo entre estas duas unidades orgânicas. Não sendo propriamente equivalentes, os conceitos utilizados resultaram de diferentes leituras do que se entende por gestão de processos ou abordagem por processos. No entanto, os diferentes modelos conceptuais encontrados, independentemente do nível de granularidade dos processos levantados, acabam por coincidir na representação daquilo que são as funções da administração pública, permitindo assim o seu mapeamento, ainda que não de forma linear.

Quadro 1 – Equivalência dos conceitos utilizados

CONCEITOS	SIGNIFICADO atribuído		CONCEITOS
	DMRH	**DAM**	
Macroprocesso	Grande conjunto de atividades (processos) por meio dos quais a organização cumpre a sua missão, gerando valor. Geralmente corresponde a uma função-chave da organização.	1.º Nível na MEF e na Lista Consolidada. As funções correspondem aos grandes domínios da ação mandatada ao sector público.	**Função**
Processo	É um conjunto de atividades que transforma entradas (*inputs*) em resultados ou saídas (*outputs*) e, deste modo, acrescenta valor.	3.º Nível na Lista Consolidada. Um processo de negócio corresponde a uma sucessão ordenada de atividades interligadas, desempenhadas para atingir um resultado definido (produto ou serviço), no âmbito de uma subfunção.	**Processo de Negócio (PN)**
Subprocesso	Processo integrado noutro processo, ou seja, é uma subdivisão desse outro processo	Na LC um PN pode decompor-se em duas ou mais subdivisões em razão das decisões de avaliação.	**4.º Nível**
Atividade	Conjunto de tarefas necessárias para a obtenção de um resultado.	Partes que constituem os processos, desempenhadas por participantes e que acrescentam valor.	**Atividades**
Processos estratégicos e de regulação [ou de gestão]	Destinam-se controlar as políticas, estratégias e metas de uma organização. Estão intimamente relacionados com a visão e a missão. Envolvem a gestão de topo e afetam a totalidade da organização.	Funções de Apoio à Governação – centradas na Estratégia, Planeamento e Controlo de Gestão. Realização das missões operacionais.	**Funções de apoio à governação** **Funções normativa, reguladora e fiscalizadora**
Processos operacionais [ou de realização ou de negócio]	São os que geram os produtos/ serviços disponibilizados ou prestados aos/às clientes. Genericamente compreendem as funções de conceção, produção e distribuição de um produto. São por vezes designados processos-chave ou considerados como parte destes.	Realização das missões operacionais.	**Funções produtiva e prestadora de serviço**
Processos de suporte [ou de apoio]	Compreendem as atividades (internas e geralmente transversais) necessárias ao correto funcionamento dos processos operacionais.	Funções de suporte à gestão de recursos – centradas na gestão dos recursos complementares, mas necessários à realização das Missões Operacionais.	**Funções de suporte à gestão de recursos**

Da dinâmica gerada ao longo das várias sessões em que se (co)elaborou a nova arquitetura dos macroprocessos da DMRH (Fig. 1) e, na sequência desta, a nova versão do Catálogo de Processos, emergiram algumas opções e constatações que importa destacar:

- Na identificação dos macroprocessos, processos e subprocessos da DMRH, procurou-se articular a perspetiva da Gestão de Recursos Humanos com o modelo conceptual dos domínios/funções/subfunções e processos de negócio representado na Lista Consolidada.
- As diferentes interpretações a nível dos conceitos e a granularidade de muitos dos processos/procedimentos sinalizados para integração no Catálogo foram as principais dificuldades sentidas nesse esforço de adequação.

- Também já foi iniciado o mapeamento dos processos constantes no Catálogo de Processos da DMRH aos processos de negócio da Lista Consolidada, por forma a permitir a atribuição de prazos de conservação administrativa e destinos finais aos processos levantados.
- Na sequência destas reuniões, após discussão de uma primeira proposta de mapeamento com os serviços donos dos processos, foram recomendadas algumas alterações à lista dos processos de negócio incluídos na Tabela de Seleção, parte integrante da proposta de Portaria de Gestão de Documentos para as Autarquias Locais, em fase de aprovação.
- Será ainda necessário realizar reuniões com as unidades orgânicas responsáveis pela reorganização dos seus processos para pode retirar dúvidas concretas que os mapeamentos têm suscitado.
-

Figura 1- Arquitetura de macroprocessos da DMRH

Fonte: Direção Municipal de Recursos Humanos da Camara Municipal de Lisboa

O Quadro 2 apresenta alguns exemplos das correspondências estabelecidas entre o Catálogo de Processos da DMRH e a LC.

Quadro 2 - Alguns exemplos dos mapeamentos

Título do assunto/ processo	Descrição do assunto/ processo	Código	Título	Descrição	PCA	Forma de contagem	DF
Re(definir) o catálogo de processos da DMRH	Catálogo de processos da DMRH	**150.20.500**	Análise e melhoria de processos	Definição de procedimentos e processos administrativos com vista à implementação de boas práticas e melhoria da qualidade dos serviços. Inicia com o estudo do processo e termina com implementação de circuito estruturado, independentemente do suporte de informação. Inclui identificação de etapas do processo administrativo, estudo de regulamentos e de legislação relacionada, definição de requisitos e normalização de formulários.	10	F04	E
Realizar estágios curriculares	Estágio Curricular	**750.20.600**	Realização de atividades de ensino ou formação	Concretização de atividades formativas, letivas e extra curriculares. Inicia com a análise do programa de curso ou formação e termina com a apresentação do relatório sobre a concretização das atividades curriculares letivas e formativas no encerramento da ação ou do ano letivo. Inclui elaboração de plano de aula ou plano de formação, implementação de estratégias técnico-pedagógicas, definição de planos de recuperação, de acompanhamento ou desenvolvimento, produção de sumários, elaboração de relatórios periódicos das aulas, apresentação de propostas de atividades, monitorização do desenvolvimento das aprendizagens e interação entre docentes ou formadores e alunos ou formandos.			

Eixo 2 – Documentação e otimização do "Processo individual" do trabalhador/a

No âmbito dos processos de avaliação de documentos acumulados levados a cabo, a solicitação das unidades orgânicas, a DAM constatou que apareciam, com frequência, conjuntos de documentos com informação relativa aos trabalhadores e trabalhadoras que eram sempre designados por "processos individuais". A questão levantada por este conjunto documental, que tendo esta designação teria de ser considerado de conservação definitiva, conduziu à necessidade de analisar o seu conteúdo para entender se estávamos perante uma duplicação dos mesmos documentos que já constavam nos "processos individuais" existentes na DMRH e constituiu um impulso determinante para a aproximação entre as duas unidades orgânicas.

A DAM, após uma análise dos documentos existentes nestes conjuntos documentais, questionou a pertinência da sua conservação, tendo em conta que se tratava, na sua grande maioria, de justificação de faltas e outros documentos relacionados com o controlo de assiduidade dos/as trabalhadores/as nas respetivas unidades orgânicas por onde passavam ao longo do seu percurso profissional no Município de Lisboa.

Por iniciativa da DAM, em julho de 2018, realizou-se a primeira reunião com a DMRH "dona do negócio", para tomar uma decisão sobre o destino final a dar a estes documentos, a conservação ou a eliminação). Concluindo-se que se tratava da atribuição da mesma designação a realidades distintas e que esta situação tinha conduzido à existência de um elevado volume de informação duplicada, foi produzido um despacho conjunto do Diretor Municipal da Cultura e do Diretor Municipal de Recursos Humanos, onde, entre outros aspetos, se esclarece que:

- O Processo Individual do funcionário/a é apenas aquele que é constituído e gerido na DMRH.
- Toda a documentação pertinente para a salvaguarda dos direitos e dos deveres do/a funcionário/a deve ser remetida para a DMRH, não devendo ser conservada cópia no serviço onde aquele desempenha funções.
- Considerando que as atividades de suporte ao processamento de controlo de assiduidade dos/as trabalhadores/as, é uma competência delegada pela DMRH nos serviços municipais, os quais desta forma participam no procedimento estabelecido para a gestão das férias e faltas, deve ser conservada no serviço onde o funcionário/a desempenha funções, apenas a documentação relativa ao controlo de assiduidade.
- Os processos constituídos nos serviços para guardar a documentação relativa ao controlo de assiduidade dos trabalhadores/as que aí desempenham funções, não devem ser designados de processos individuais, mas antes de "Processos de controlo de assiduidade".

A clarificação da finalidade e características (designadamente os prazos de conservação) destes dois tipos diferenciados de conjuntos documentais levou à diferenciação e autonomização do procedimento de gestão do processo de controlo de assiduidade (desenvolvido por cada Unidade Orgânica) em relação ao procedimento de gestão do processo individual dos/as trabalhadores/as (desenvolvido exclusivamente pela DMRH).

Ambos constam do Catálogo de Processos da DMRH e estão a ser documentados e otimizados (designadamente em termos da conformidade com o RGPD) no âmbito do Projeto Gestão por Processos. Relativamente à gestão do processo individual, importa realçar que a otimização deste procedimento visa sobretudo a melhoria na racionalização e organização da informação sobre o/a trabalhador/a, atendendo a que essa informação existe, em muitos casos, também em suporte digital e ao facto do conteúdo constante de um "processo individual" ser de conservação permanente. A necessidade de otimização torna-se evidente face ao crescimento acentuado deste volume documental: entre 2016 e 2018, foram atualizados 54.916 processos individuais com inserção de 317.411 folhas, o que corresponde a uma média anual de 18.305 processos individuais atualizados e 105.804 folhas[7], ou seja, a um crescimento anual médio de 116,6 metros lineares[8].

Este eixo de intervenção teve já um efeito positivo no ciclo de vida do próprio processo individual dos/as trabalhadores/as desvinculados do Município que se encontram sob custódia da DAM, considerados de conservação permanente: está em curso uma reavaliação de um conjunto de processos que, sendo afinal processos de controlo de assiduidade, poderão ser eliminados.

Eixo 3 - Documentação e otimização do "Processo de controlo de assiduidade" do trabalhador/a.

Desde março a agosto de 2019, os/as técnicos/as da DAM estiveram presentes em seis reuniões conjuntas com a equipa da DMRH, com a finalidade de definir o conteúdo e as práticas necessárias à gestão adequada do "Processo de Controlo de Assiduidade", o qual no Catálogo de Processos da DMRH corresponde ao procedimento PO6.AP-P1 Gerir o "processo" de controlo de assiduidade.

Durante a fase de levantamento de informações sobre este procedimento, foram realizados testes comparativos entre os processos de controlo de assiduidade existentes em duas unidades orgânicas e os "correspondentes" processos individuais geridos pela DMRH. Estes comprovaram que os processos de controlo de assiduidade, de um modo geral, não contêm documentos pertinentes para a salvaguarda dos direitos e dos deveres do/a funcionário/a.

Para garantir a implementação nas unidades orgânicas de procedimentos adequadas ao nível da gestão dos processos de controlo de assiduidade foi elaborada uma Ficha de Orientação técnica explicitando:

- O que é o Processo de Controlo de Assiduidade.
- Como constituir o Processo de Controlo de Assiduidade
- Como manter atualizado o Processo de Controlo de Assiduidade
- Como eliminar documentos relativos ao controlo de assiduidade

[7] Dados fornecidos pelo Núcleo de Arquivo da Divisão de Gestão de Processo e Remuneração/DGRH/DMRH, em 2-10-2019.

[8] Para esta estimativa, tomou-se como base a altura de uma resma de papel A4 (500 folhas): 55 cm.

Estas orientações técnicas foram testadas numa Direção Municipal entre julho e setembro deste ano e irão ser divulgadas pelas/os interlocutores de recursos humanos (Função RH) em todas as Direções Municipais com vista à sua operacionalização.

4. Conclusão

Conclui-se que a metodologia adotada permite obter resultados práticos de forma mais eficiente, estimulando o inter-relacionamento organizacional e a partilha de conhecimento especializado. Cada membro da equipa colaborativa trouxe consigo as suas forças, aptidões, experiências e habilidades únicas para dar corpo e cumprir o objetivo comum enquadrado numa perspetiva de Gestão de Informação e de proteção de dados pessoais.

A experiência colaborativa desenvolvida entre a DMRH e DAM revelou-se particularmente útil para a implementação setorial do RGPD na CML e, sobretudo, para a melhoria organizacional através introdução da perspetiva de "ciclo de vida dos documentos" nos processo otimizados e, em particular, da aplicação de prazos de conservação administrativa e destino final (conservação definitiva ou eliminação).

Em suma, o RGPD está a revelar-se uma excelente oportunidade na componente da gestão da mudança e inovação organizacional no Município de Lisboa.

5. Referências bibliográficas

COLLIS, J.; HUSSEY, R. – **Pesquisa em Administração: um guia prático para alunos de graduação e pós-graduação**. 2ª ed. Porto Alegre: Bookman, 2005.

DECISÃO (UE) 2015/2240 DO PARLAMENTO EUROPEU E DO CONSELHO, de 25 de novembro de 2015, que cria um programa sobre soluções de interoperabilidade e quadros comuns para as administrações públicas, as empresas e os cidadãos europeus (Programa ISA2) como um meio para modernizar o setor público. *JOUE*, L n. 318. [Em linha]. Disponível na Internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015D2240&from=EN>.

DELIBERAÇÃO N.º 305/AML/2018: ajustamento à orgânica dos Serviços Municipais do Município de Lisboa. Boletim Municipal, n. 1279, 1.º Suplemento. [Em linha]. Lisboa: IML, 2018. [Consult. 13 ago. 2019]. Disponível na Internet: <URL:http://www.cm-lisboa.pt/municipio/boletim-municipal>.

DELIBERAÇÃO N.º 288/CM/2018: criação da Equipa de Projeto para a Implementação do Regulamento Geral de Proteção de Dados. Boletim Municipal, n. 1267, 5º Suplemento [Em linha]. Lisboa: IML, 2018, p. 240-245. [Consult. 13 ago. 2019]. Disponível na Internet: <URL:http://www.cm-lisboa.pt/municipio/boletim-municipal>.

DIREÇÃO-GERAL DO LIVRO, DOS ARQUIVOS E DAS BIBLIOTECAS – **Orientações básicas para o desenvolvimento dos 3ºs níveis em planos de classificação conformes à Macroestrutura Funcional**. [Em linha]. Lisboa: DGLAB, 2013. [Consult. 30 de maio de 2019].

Disponível na Internet: <URL: http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2014/02/2013_Orient-3-niveis_PC-MF.pdf>.

DIREÇÃO-GERAL DO LIVRO, DOS ARQUIVOS E DAS BIBLIOTECAS – ***Avaliação Suprainstitucional da Informação Arquivística (ASIA): documento metodológico.*** [Em linha]. Lisboa: DGLAB, 2016. [Consult. 30 maio 2019]. Disponível na Internet: <URL:http://arquivos.dglab.gov.pt/wp-content/uploads/sites/16/2016/03/ASIA_Doc-metodologico2016-03-10.pdf>.

DIREÇÃO-GERAL DO LIVRO, DOS ARQUIVOS E DAS BIBLIOTECAS – ***Lista Consolidada para a classificação e avaliação da informação pública (LC)*.** [Em linha]. Lisboa: DGLAB, 2019. [Consult. 13 ago. 2019]. Disponível na Internet: <URL:http://arquivos.dglab.gov.pt/programas-e-projectos/modernizacao-administrativa/macroestrutura-funcional-mef/lista-consolidada/>.

DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS – **Plano de Atividades 2019**. [Lisboa: DMRH]. [Consult. 13 set. 2019]. Disponível na Internet: <URL:http://www.cm-lisboa.pt/fileadmin/MUNICIPIO/Camara_Municipal/Transparencia/ProgramasRelatorios2019/PA_DMRH_2019.pdf>.

DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS (2018) – **Quadro de Avaliação e Responsabilização para 2018**. [Em linha]. [Lisboa: DMRH]. [Consult. 13 set. 2019]. Disponível na Internet: <URL:http://www.cm-lisboa.pt/fileadmin/MUNICIPIO/Camara_Municipal/Transparencia/ProgramasRelatorios2018/QUAR_DMRH_2018.pdf>.

DIREÇÃO MUNICIPAL DE RECURSOS HUMANOS – **Projeto Gestão por Processos 2.0: proposta de (re)lançamento do projeto: plano de ação**. Lisboa: DMRH. Versão 1 [30-1-2019].

FREIRE, M. – RGPD: empresas ainda não estão m conformidade total. **Business.IT.** [Em linha]. 6 set. 2019. [Consult. 12 set. 2019]. Disponível na Internet: <URL:https://business-it.pt/2019/09/06/rgpd-empresas-ainda-nao-estao-em-conformidade-total/>.

LOURENÇO, A.; PENTEADO, P. – **A caminho da ASIA: Avaliação Suprainstitucional da Informação Arquivística**. In Congresso Nacional de Bibliotecários e Arquivistas, 12, Évora, 2015. *Ligar. Transformar. Criar valor"*. [Em linha]. Lisboa: BAD, 2015. [Consult. 30 de maio de 2019]. Disponível na Internet: <URL: https://www.bad.pt/publicacoes/index.php/congressosbad/article/view/1458/pdf_90>.

LOURENÇO, A.; PENTEADO, P.; GAGO, R. – **A Lista Consolidada como instrumento facilitador de aplicação do RGPD**. In JORNADAS GESTÃO DE INFORMAÇÃO, 2, Ponte da Barca, 2018. *Interação entre arquivistas e informáticos*. [Em linha]. [Consult. 13 ago. 2019]. Disponível na Internet: <URL: https://www.bad.pt/eventos/wp-content/uploads/2018/01/P.-Barca_LC_CLAV_RGPD_v2.pdf>.

NP 4438-1. Gestão de documentos de arquivo. Parte 1: Princípios diretores. Lisboa: Instituto Português da Qualidade: Lisboa: IPQ, 2005.

NP 4438-2:2005. Gestão de documentos de arquivo. Parte 2: Recomendações de aplicação. Lisboa: Instituto Português da Qualidade, 2005.

NP EN ISO 9001:2015. Sistemas de Gestão da Qualidade: requisitos. Lisboa: Instituto Português da Qualidade, 2015.

PORTARIA N.º 412/2001, de 17 de abril. Diário da República, I série-B, n. 90, p. 2243-2260. [Em linha]. [Consult. 13 ago. 2019]. Disponível na Internet: <URL: https://dre.pt/application/file/a/164160>.

PORTARIA N.º 1253/2009, de 14 de outubro. Diário da República, I série, n. 199, p. 7635-7649. [Em linha]. [Consult. 13 ago. 2019]. Disponível na Internet: <URL:https://dre.pt/application/file/a/491579>.

REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). JOUE, L n. 119, p.1-88. [Em linha]. Disponível na Internet: <URL:https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT>.

REIS, D.; FERREIRA, M. A. – Um ano depois: a aplicação do RGPD e as ferramentas de marketing. Meios & publicidade. [Em linha], 1 jul. 2019. [Consult. 12 set. 2019]. Disponível na Internet: <URL: http://www.meiosepublicidade.pt/2019/07/um-ano-aplicacao-do-rgpd-as-ferramentas-marketing/>.

WILSON, T. D. – **Information management. In International Encyclopaedia of Information and Library Science**. 2nd. London: Routledge, 2002. pp. 263-278.

YIN, R. K. – **Estudo de caso: planejamento e métodos**. 2ª ed. Porto Alegre: Bookman, 2001. Também disponível em: http://pt.scribd.com/doc/46546362/Estudo-de-Caso-to-e-Metodos-Robert-k-Yin.

O Consumerismo e os Problemas Socioambientais na Sociedade Moderna: Por uma Sustentabilidade Socioecológica[9]

Cleide Calgaro[10]
Agostinho Oli Koppe Pereira[11]

RESUMO

No presente trabalho estabelece-se como problema: como é possível vislumbrar uma sustentabilidade socioecológica na sociedade moderna? A base para a solução do problema está no estudo do consumocentrismo e dos problemas socioambientais por ele criados. O método utilizado é o analítico, partindo de premissas da realidade socioambiental atual com base em estudos bibliográficos que trabalham com a questão proposta. Conclui-se que é possível se vislumbrar a sustentabilidade socioecológica a partir de algumas alternativas, sendo elas: a mudança de racionalidade, a educação e a conscientização dos seres humanos, juntamente com o decrescimento e o bem viver. Desse modo, os ciclos vitais da natureza e a sociedade podem ser preservados e mesmo restaurados. Isso permite que haja a harmonia e a interconexão entre ser humano e meio ambiente, minimizando os problemas socioambientais causados pela sociedade consumocentrista capitalista moderna.

PALAVRAS-CHAVE

Consumocentrismo; problemas socioambientais; sustentabilidade socioecológica; modernidade.

[9] Trabalho financiado pelo Edital 2/2017 da FAPERGS, resultante dos Grupos de Pesquisas (CNPQ): Metamorfose Jurídica, Regulação Ambiental da Atividade Econômica Sustentável (REGA) e Filosofia do Direito e Pensamento Político (UFPB).

[10] Pós-Doutora em Filosofia e em Direito ambos pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Doutora em Ciências Sociais na Universidade do Vale do Rio dos Sinos - UNISINOS. Doutora em Filosofia pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Doutora em Direito pela Universidade de Santa Cruz do Sul – UNISC. Atualmente é Professora da Graduação e Pós-Graduação - Mestrado e Doutorado - em Direito na Universidade de Caxias do Sul - UCS. É Líder do Grupo de Pesquisa "Metamorfose Jurídica" vinculado a Universidade de Caxias do Sul-UCS. Orcid: https://orcid.org/0000-0002-1840-9598. CV: http://lattes.cnpq.br/8547639191475261. E-mail: ccalgaro1@hotmail.com

[11] Doutor em Direito pela Universidade do Vale do Rio dos Sinos (2002). Pós-doutor em Direito pela Universidade do Vale do Rio dos Sinos - UNISINOS. Mestre em Direito pela Universidade Federal de Pernambuco (1986). Especialista em Metodologia do Ensino e da Pesquisa Jurídica pela Universidade de Caxias do Sul (1984). Graduado em Direito pela Universidade de Caxias do Sul (1978). Atualmente é professor colaborador na Universidade de Passo Fundo - UPF, atuando no Curso de Mestrado em Direito. Orcid: https://orcid.org/0000-0003-2939-7534. CV: http://lattes.cnpq.br/5863337218571012. E-mail: agostinho.koppe@gmail.com

Consumerism and Social and Environmental Problems in Modern Society: Towards Sociecological Sustainability

ABSTRACT

In the present work, the problem is established: how is it possible to envision a socio-ecological sustainability in modern society? The basis for solving the problem lies in the study of consumptioncentrism and the socio-environmental problems it creates. The method used is analytical, starting from assumptions of the current socio-environmental reality based on bibliographic studies that work with the proposed question. It is concluded that it is possible to glimpse the socio-ecological sustainability from some alternatives, namely: a change in rationality, education and awareness of human beings, together with degrowth and good living. In this way, the life cycles of nature and society can be preserved and even restored. This allows for harmony and interconnection between human beings and the environment, minimizing the socio-environmental problems caused by the modern capitalist consumer-centrist society.

Keywords: Consumerocentrism, social and environmental problems; socioecological sustainability; modernity.

Introdução

No presente trabalho pretende-se verificar como o progresso e o consumocentrismo na sociedade moderna criam os problemas socioambientais estabelecendo a insustentabilidade socioecológica. Nesse contexto pretende-se verificar como seria possível se vislumbrar uma sustentabilidade socioecológica, ou seja, uma sustentabilidade preocupada como o meio ambiente e os seres vivos que habitam o Planeta, permitindo uma interligação e interconexão entre ambos. Busca-se entender como se pode criar uma sustentabilidade socioecológica apesar dos moldes capitalistas, pautados no progresso tecnológico e na dominação de mercado pelas grandes corporações e pelo capital. Outro problema, que se infere no texto, é como o consumo, que se coloca no centro da sociedade – sociedade consumocentrista – pode ser repensado nos atuais contextos existentes, uma vez que adestra e dociliza os sujeitos.

Para o enfrentamento de tais questionamentos utiliza-se o método analítico, tendo como base o estudo de referências acerca da temática proposta para, ao final, apresentar os resultados levantados a partir dos estudos enfocados.

Inicia-se o trabalho estudando a sociedade consumocentrista, dentro da estrutura da modernidade, que se pauta num progresso tecnológico, mas não se preocupa com os problemas socioambientais, que são prementes na atualidade. Tais problemas podem ser especificados como: os sociais – desigualdade, pobreza, etc. - e ambientais – poluição do ar, das águas e das áreas de terras, aquecimento global, chuvas ácidas, etc. -

Num segundo momento, se estabelece o que é a sustentabilidade socioecológica e como a mesma pode ser uma alternativa para o quadro que se delineou anteriormente na conjuntura moderna atual. Dessa forma, também, se traz algumas alternativas pontuais a fim de possibilitar a sustentabilidade que é proposta.

Com isso, conclui-se que, para se atingir uma sustentabilidade socioecológica, é preciso uma nova racionalidade humana, na qual o ser humano, enquanto indivíduo, busque se colocar no lugar do outro e da natureza, sendo que, este mesmo ser humano, enquanto coletividade se posicione dentro de parâmetros sociais humanitários e, ao mesmo tempo, preservacionistas em termos globais. Para tal são necessárias: a conscientização, a participação, a solidariedade e a alteridade, nas quais as pessoas resgatem o sentimento de pertencimento aos espaços em que vivem e se busque um ideal de comunidade.

1. Sociedade Consumocentrista, Progresso e os Problemas Socioambientais na Modernidade

A sociedade moderna se pauta no hiperconsumo, ou seja, um consumismo exagerado que leva as pessoas a atrelarem a sua felicidade a um molde de vida fútil e individualista. O progresso tecnológico permitiu que as sociedades evoluíssem em criação de bens e, através destes idealizou-se um constructo social capaz de tornar as pessoas dependentes do consumo dos mesmos. Com a dependência veio o adestramento, direcionando o pensamento do indivíduo para o consumo. Surge uma sociedade, na modernidade, a qual o consumo se torna o centro dela, a sociedade consumocentrista. Desta forma, é importante se entender a modernidade, que na ótica de Pereira *et al.*, "veio, com a possibilidade, por meio de conceitos concretos e desenvolvidos sob a ótica das certezas tecnológicas e científicas, além, certamente, da utilização da razão como forma de dominação da natureza, estabelecer uma sociedade capaz de proporcionar felicidade e satisfação a todos os cidadãos. [...]" (PEREIRA; PEREIRA, 2008, p.230). Denotam ainda que "com a modernidade, surgem aspectos como o dinamismo tecnológico, a forte vinculação com a razão; a idéia de ciência, como elemento de exatidão e certeza; a liberdade vinculada à razão; o otimismo exagerado de benesses a todos, dentro da idéia de globalização, entre outros". (PEREIRA; PEREIRA, 2008, p.230).

Essa modernidade trouxe a dominação tanto do ser humano como da natureza, sendo que ela se atrelou ao capitalismo em nome da razão. Para Bauman (1999, p.18) a modernidade "[...] é o que é – uma obsessiva marcha adiante – não porque nunca consegue o bastante; não porque se torne mais ambiciosa e aventureira, mas porque suas aventuras são mais amargas e suas ambições mais frustradas".

Da modernidade emerge o individualismo, sendo uma nova ordem social e cultural, ditando modelos e modas, credos e religiões, culturas e padrões, por fim, ditando a religião[12] do consumo. Para Lyon o termo modernidade "se aplica à ordem social que emergiu depois do Iluminismo. Embora suas raízes se estendam até épocas bem anteriores ao Iluminismo, o mundo do moderno está marcado por seu dinamismo sem precedentes, por sua rejeição da tradição, ou sua marginalização, e por suas consequências globais". (LYON, 1998, p. 35). Já para Giddens, "a modernidade refere-se a estilo, costume de vida

[12] Quando se fala em religião, não se discute crença religiosa e, sim, instituições. Nesse contexto se traz a religião como uma instituição a qual as pessoas possuem a crença na existência de um poder ou princípio superior, que no caso é o consumo e suas facilidades, se tornando dependentes além de devotarem seu respeito e sua obediência na sociedade moderna. As pessoas têm tanta fé no consumo que atrelam sua vida e sua felicidade ao mesmo.

ou organização social que emergiram na Europa a partir do século XVII e que ulteriormente se tornaram mais ou menos mundiais em sua influência". (GIDDENS, 1991, p. 11.)

David Harvey entende que a modernidade, "por conseguinte, não apenas envolve uma implacável ruptura com todas e quaisquer condições históricas precedentes, como é caracterizada por um interminável processo de rupturas e fragmentações internas inerentes". (2009, p. 22). Na visão de Stuart Hall, "as sociedades modernas são, portanto, por definição, sociedades de mudanças constantes, rápidas e permanentes. Essa é a principal distinção entre as sociedades "tradicionais" e as sociedades "modernas"" (2014, p.04).

Com isso a sociedade consumocentrista acaba sendo uma sociedade entrelaçada com a modernidade e, neste entrelaçamento determina-se que o consumo seja o centro das atenções, templo de culto e adoração. As pessoas se tornam mais individualistas e adestradas aos moldes do que as grandes corporações querem inserir no mercado. O mercado capitalista busca a valorização do modelo econômico pautado na expropriação e exploração dos recursos naturais e humanos. A vida gira na compulsão pelo consumo, seja de bens ou de novas tecnologias, que surgem como fenômeno de dominação e adestramentos dos sujeitos.

Para Pereira e Calgaro "na atualidade, as pessoas não consomem mais por necessidade, mas sim pelo prazer de comprar, seja para satisfazer suas futilidades, ou simplesmente, por consumir" (PEREIRA; CALGARO, 2015, p. 16). Assim sendo as pessoas voltam sua felicidade, seus sonhos e sua vida à arte do consumo e esse consumo acaba sendo o centro da vida e das atenções dentro do contexto social.

Portanto, se vive numa era consumocentrista, na qual as relações dos sujeitos são ligadas por mercadorias e objetos, as pessoas preferem as tecnologias para se comunicarem e se individualizarem e, já não mais se reúnem em grupos sociais, perdendo o espírito de solidariedade e de comunidade. Os valores funcionais dos objetos fazem com que as pessoas se sintam pertencentes a um mundo que é dinâmico e que sempre apresenta novos atrativos e condições, por exemplo, novos celulares, carros, computadores, etc., que fazem com que esses sujeitos se docilizem e se adestrem a um modo de vida heteronomamente criado. Essa vida, criada pelo mercado, leva a uma escravidão tecnológica e a uma moda inventada, sendo que as pessoas, nas maiorias das vezes, não precisam desses objetos, mas os compram a fim de se sentirem pertencentes à

sociedade moderna consumocentrista[13]. Nesse sentido Pereira e Calgaro (2014, p.14) assinalam que "essa cultura consumista se desenvolve, também, a partir de uma educação que cria o desejo pelo consumo, pelo descarte, pela valorização do novo. O velho se torna ultrapassado e sem sentido. Porém, as consequências dessas atitudes não têm qualquer proeminência para o "ser consumidor"". Portanto, "consumir se torna a palavra mágica, capaz de transformar a vida do indivíduo, alçando-o ao patamar de detentor de *status* e de poder no mundo, fazendo com que este se sinta grandioso, o "deus" de possibilidades e de oportunidades". (PEREIRA; CALGARO, 2014, p. 14).

Dessa forma, o consumo criado na modernidade acaba sendo hiperconsumismo, sendo, o cidadão, dessubjetificado e perdendo sua própria identidade. Perdendo sua identidade já não com o seu ser e com as consequências dos seus atos hiperconsumistas. Nesse diapasão só se interessa com o consumo, não se preocupando com os danos socioambientais de seus atos. Compra em excesso, logo descarta em, ou seja, um consumo exagerado e excessivo se necessidade. Rede essa, que desvaloriza a cultura do ser e se baseia no aparentar, levando as pessoas viverem através de máscaras sociais e pessoais, não consistindo em o que gostariam de ser e, sim, no que os outros ou mesmo a sociedade lhes impõem. A frustração, a depressão, a dependência são fatores marcantes na sociedade consumocentrista, a qual dita valores de felicidade e de saciabilidade dos desejos, que são forjados pelo progresso, pelo mercado, pela cultura comercial e pelas grandes corporações. Dita-se os moldes de vida, os padrões de família, a cultura, etc., com isso, o sujeito acaba vivendo um teatro[14] mascarando seus reais desejos e anseios. Campbell (2007, p.53) afirma que "eu compro a fim de descobrir quem sou". A partir dessa afirmação, se observa que, o ser humano compra para existir socialmente e sua vida se atrela a essa máscara de consumo, na qual a felicidade está conectada. Eu compro a fim

[13] Todos os dias parece que o mundo do consumo se imiscui em nossas vidas e modifica nossas relações com os objetos e com os seres, sem que, apesar disso e das críticas que se formulam a respeito dele, consiga-se propor um contramodelo crível. E, para além da postura crítica, seriam raros aqueles que desejariam mesmo aboli-lo em definitivo. É forçoso constatar que seu império não pára de avançar: o princípio de *self-service*, a busca de emoções e prazeres, o cálculo utilitarista, a superficialidade dos vínculos parece ter contaminado o conjunto do corpo social, sem que nem mesmo a espiritualidade escape disso. (LIPOVETSKY, 2004, p.33).

[14] Erving Goffman nasceu em 11 de junho de 1922, foi sociólogo e escritor. Publicou o livro "A representação do eu na vida cotidiana" sendo que estuda as máscaras que cada um desempenha dentro do contexto social, ou seja, faz disso uma metáfora da vida social como um teatro, onde cada um desempenha um papel. Goffman tem como centro de estudo a relação entre os conceitos de "performance e fachada", deste modo, o autor atua em uma posição a qual existe palco e bastidores, ou seja, existe uma encenação que cada um vive diuturnamente em suas vidas. Goffman situa os elementos da atuação em consideração, sendo assim, um ator pode atuar na posição na qual há o palco e mesmo onde existam bastidores. Desta forma, existe uma relação entre a peça e a sua atuação e, o ator está sendo visto por um público, mas ao mesmo tempo, esse mesmo ator é o público da peça encenada pelos espectadores. (GOFFMAN, 2014).

de aparentar ser e ter na sociedade, a qual impõe seus padrões e moldes de vida, de felicidade, de relacionamentos, etc., pois se eu comprar eu existo, sou alguém no meio da multidão global. Desse modo, se eu compro, logo vou existir na sociedade consumocentrista.

Para Pereira e Calgaro "essa felicidade é incognoscível, pois, no fundamento do mercado moderno, ela deve ser sempre procurada e nunca é saciada. Na atualidade a fórmula do consumo é: buscar uma felicidade que, ao ser tocada, evanesce e esmorece para que ela seja buscada novamente e continuamente todos os dias". (PEREIRA; CALGARO, 2014, p. 13). Dessa maneira, "o consumismo é global, não no sentido de que todos podem consumir, mas no de que todos são afetados por ele" (LYON, 1998, p.104). Entende-se que a sociedade deixa de ser somente sociedade de consumo, perpassando do consumismo ao hiperconsumismo, até chegar ao consumo como centro da mesma, se tornando uma sociedade consumocentrista pautada na ordem do progresso e da modernidade. Pereira et. al. denotam que:

> A sociedade vivenciou uma série de teorias ao longo do tempo, o que faz com que as condutas humanas fossem dirigidas por certas teorias/doutrinas/ideias/ideologias, que levavam a mudanças sociais e individuais. Pode-se destacar, de modo exemplificativo, dentro do contexto que se está abordando, o cosmocentrismo (o cosmos é o centro de tudo); o teocentrismo (Deus se torna o centro); o antropocentrismo (tudo gira em torno do homem). Na sociedade moderna contemporânea que já está sendo denominada de pós-moderna, conforme se pretende demonstrar aqui, se insere o consumocentrismo, como elemento dominante para onde se dirigem o pensamento e as atividades do cidadão moderno, fazendo com que o mesmo seja levado a consumir, pois, através desse ato, ele se realiza como ser individual e social, pois que ele somente é se consumir. (PEREIRA; CALGARO; PEREIRA, 2016, p. 267).

Assim, a sociedade consumocentrista se molda no fato de que "o consumo se coloca no centro de todas as decisões que envolvem o indivíduo, pois o mesmo perde sua identidade como ser que participa das decisões sociais para se transformar (apenas) em consumidor heteronomamente guiado". (PEREIRA; CALGARO; PEREIRA, 2016, p. 267). Os mesmos autores prosseguem o sentido de consumocentrismo demonstrando que: "entende-se que se ultrapassou a denominada sociedade hiperconsumista, dando azo a uma sociedade consumocentrista. Nesse viés, o consumo passa a ser o elemento principal das atividades humanas, deslocando o ser para o ter e, posteriormente, para o aparentar" (PEREIRA; CALGARO; PEREIRA, 2016, p. 267). Portanto: "o consumo se torna o centro da sociedade contemporânea, onde o consumidor vai buscar todas as possibilidades

de sua nova razão de viver. Consumir é existir". (PEREIRA; CALGARO; PEREIRA, 2016, p. 267).

Com base nessa lógica, o consumocentrismo acaba sendo o centro da sociedade e o representante da religião do momento, ou seja, se torna o "Deus" da modernidade, o qual tudo provê. Com isso os sujeitos acabam integrando as formas hiperconsumista a sua vida e aos seus hábitos, moldando os seus padrões e seu convencimento. Dentro dessa concepção "se o sujeito não participa desse "jogo já jogado" da sociedade consumocentrista, será excluído, perfazendo para o sujeito aquilo que se pode denominar de "morte social".

Outro aspecto que se vem abordando e que ocorre na sociedade consumocentrista é a dessubjetivação do sujeito, ou seja, o apagamento de sua subjetividade. Na questão referente ao consumo a dessubjetivação é a objetificação do sujeito. Para melhor entendimento pode-se afirmar que a existência do indivíduo gira em torno do consumo o que fazer com que o consumo se impregne ao indivíduo, tornando-o alheio ao seu contexto social que fuja ao consumir. Assim para esse indivíduo consumocentrista a degradação ambiental e as demais situações sociais não possuem nenhum interesse. Por esses cominhos o indivíduo esquece-se de quem ele é, enquanto ser social, e se confunde com o objeto próprio de consumo. O sujeito existe para a vida moderna pensando que comanda e possui os seus rumos e os da sociedade, mas não percebe o quanto é adestrado e docilizado pelo mercado de consumo[15].

Para Schneider (1986, p.35) "(...) por trás de cada produto que o mercado oferece encontramos a diferenciação da classe social a que o mesmo se destina. Cada produto na sociedade de consumo simboliza alguma coisa". Portanto, o estilo de vida refere-se a um padrão de consumo que reflete as escolhas de uma pessoa sobre como gastar seu tempo e dinheiro. Em um sentido econômico, o estilo de vida representa o modo escolhido para distribuir a renda, tanto em termos de diferentes produtos e serviços quanto de alternativas específicas dentro dessas categorias. (SOLOMON, 2002, p. 145-146). Debord, por sua vez, entende que a sociedade vive numa era de espetáculo, sendo

[15] Lipovestsky denota que: "Todos os dias, parece que o mundo do consumo se imiscui em nossas vidas e modifica nossas relações com os objetos e com os seres, sem que, apesar disso e das críticas que se formulam a respeito dele, consiga-se propor um contramodelo crível. E, para além da postura crítica, seriam raros aqueles que desejariam mesmo aboli-lo em definitivo. É forçoso constatar que seu império não para de avançar: o princípio de self-service, a busca de emoções e prazeres, o cálculo utilitarista, a superficialidade dos vínculos parece ter contaminado o conjunto do corpo social, sem que nem mesmo a espiritualidade escape disso". (LIPOVESTSKY, 2004, p.33.)

que “o espetáculo é o momento em que a mercadoria ocupou totalmente a vida social” (1997, p.30).

A sociedade moderna capitalista vive num faz de conta, numa fantasia a qual os problemas sociais e ambientais são esquecidos, visto que acabam não sendo problemas de ninguém. Importante frisar que os problemas socioambientais, tratados no presente trabalho, podem ser entendidos da seguinte maneira: os problemas sociais estão categorizados na desigualdade social, na pobreza, na fome, no racismo, etc.; de outra banda, os problemas ambientais estão atrelados ao descarte de produtos, às mudanças climáticas, à exploração e expropriação de recursos naturais, à poluição do ar, águas e das áreas de terras, etc.

A vida na modernidade está pautada num progresso que acredita que os recursos naturais são infinitos e que a exploração e expropriação dos mesmos podem ser feita sem nenhuma preocupação com o futuro e com o presente, tanto da natureza como da humanidade. A visão das grandes corporações e do Estado é de progresso unicamente econômico, na qual tudo pode ser feito e manipulado em nome do mesmo. Torna-se inadmissível que pessoas, em plena modernidade, passem fome e sejam relegadas a condições análogas de pobreza. Algumas perguntas já são corriqueiras, mas nunca respondidas adequadamente e com o enfrentamento adequado: quem se importa com tudo isso? Quem isso beneficia com esse sistema? Por que permitir que a desigualdade social e a pobreza se somos tão avançados tecnologicamente? Há quanto tempo se houve falar em problemas ambientais, como mudanças climáticas e poluição também sem as soluções adequadas? Quanto tempo mais se continuará a andar em círculos, vendo os mesmos problemas se repetirem de geração em geração?

São questionamentos, os quais precisam ser pensados e repensados a fim de se buscar uma nova racionalidade à visão humana, antes que seja tarde demais. A sociedade consumocentrista cria pessoas egoístas e individualistas, onde o viver em comunidade se torna mais difícil, contudo é importante salientar que algumas pessoas fogem a esse estereótipo consumocentrista e, realmente, buscam vieses de alteridade, solidariedade e sustentabilidade. A sustentabilidade é um dos caminhos para a mudança, conforme se demonstrará no próximo item.

2. A Busca de uma Sustentabilidade Sociecológica

Na presente seção analisa-se a possibilidade de se buscar uma sustentabilidade que seja pautada numa visão socioecológica, a qual permita a integração e inter-relação do ser

humano com o meio ambiente para, dessa maneira, minimizar os problemas socioambientais causados pelo progresso econômico e pelo próprio poder econômico dentro de uma sociedade ajustada ao consumocentrismo e que ainda se tem por moderna.

O ser humano está voltado a uma visão antropocentrista, ou seja, ele se acha o centro de tudo, visto que, o consumo lhe dá essa sensação de satisfação e poder. O consumo como centro da sociedade moderna leva o ser humano a dimensionar que está no topo da cadeia da evolução, vez que, ele se tornou capaz de transformar a natureza em bens econômicos, porém, dentro da sociedade consumocentrista, a evolução é apenas econômica e dentro de uma concentração de capital nas mãos de apenas parte da população.

Como visto, isso leva a uma série de problemas socioambientais, os quais precisam ser minimizados e sanados de forma urgente. Carvalho (2003, p.16) afirma que: "a ideia de domínio total impõe, numa categoria de dever moral, a subjugação do não-humano. Dominar, impor, transformar, criar novas realidades materiais parece ser uma determinação inelutável ligada ao destino de "ser humano"."

Dessa maneira o ser humano impõe a dominação sobre os demais seres transformando e criando realidades materiais e imateriais. Nesse caminho de dominação os próprios seres humanos se dividem em dominadores e dominados, perdurando o racismo, a fome e a miséria material e intelectual de grande parte da humanidade. Com isso existe a necessidade de se buscar uma alternativa para essa racionalidade criada e arraigada na sociedade, por isso se propõe a criação de uma sustentabilidade que se volte para a proteção da natureza com integração humana.

Carlos Gomes de Carvalho (2003, p. 169-170) denota que "(...), fica mais que evidenciada a fragilidade dos valores humanos e dos princípios ambientais diante do Poder e dos interesses econômicos". Para ele "a sociedade civil terá que encontrar meios para criar uma blindagem mais resistente às argúcias e artimanhas do Poder Econômico que se transmudou na verdadeira razão de Estado, quando não o próprio Estado". Contudo, "estes percalços, além de outros tipos inevitáveis de oposição, são que nos devem estimular a manter a consciência de que a ideologia de um Direito solidário e de Justiça para todos, que se encontra cristalizada no Direito Ambiental, só será realizável se buscarmos a mobilização das energias éticas do cidadão, numa participação que significará um ato vigoroso do comprometimento de sua consciência moral".

Com base nesses aspectos Guimarães entende que a crise ambiental, nos tempos atuais, coloca à prova o modelo de desenvolvimento que gerou os danos ecológicos e a

desigualdade social, caracterizando-o como "politicamente injusto, culturalmente alienado e eticamente repulsivo" (2001, p.51). Nesse contexto, é preciso buscar alternativas para se atingir a sustentabilidade, na visão de Araújo, o uso da sustentabilidade como paradigma precisa de alguns requisitos que são fundamentais à manutenção da mesma. Os requisitos consistiriam em: "a) alteração dos padrões de produção; b) redução ou substituição do uso de recursos não renováveis; c) incentivo e garantia do uso sustentável de recursos renováveis; d) respeito à capacidade de suporte dos ecossistemas; e) mudança dos padrões individuais de consumo; f) delinear ferramentas locais disponíveis" (2008, p. 24).

Observa-se que, no caso da alteração de padrões de consumo, existem algumas, alternativas que podem ser elencadas:

a) As grandes corporações deveriam se preocupar não somente com o lucro e a imposição aos consumidores de bens e serviços, mas também, terem a consciência que os recursos naturais são finitos e que a expropriação dos mesmos, de forma exagerada, levará ao caos. Como Nalini coloca "só existe economia, porque a ecologia lhe dá suporte. A ecologia permite o desenvolvimento da economia. A exaustão da primeira reverterá em desaparecimento da segunda". (2001, p.143). O discurso da sustentabilidade na visão de Leff leva

> a lutar por um crescimento sustentado, sem uma justificação rigorosa da capacidade do sistema econômico de internalizar as condições ecológicas e sociais (de sustentabilidade, eqüidade, justiça e democracia) deste processo. A ambivalência do discurso da sustentabilidade surge da polissemia do termo *sustainability*, que integra dois significados: um, que se traduz em castelhano como *sustentable*, que implica a internalização das condições ecológicas de suporte do processo econômico, outro, que aduz a durabilidade do próprio processo econômico. Neste sentido, a sustentabilidade ecológica constitui uma condição da sustentabilidade do processo econômico. (grifo do autor). (LEFF, 2002, p.19-20).

b) Redução ou substituição do uso de recursos não renováveis, com incentivo e garantia do uso sustentável de recursos renováveis. O esgotamento dos recursos naturais traz junto a modificação do habitat, com a perda da diversidade biológica, que é geradora da vida como a conhecemos. Assim, reduzir a utilização de recursos não renováveis ou substituí-los por recurso renováveis – dentro de uma utilização sustentável – é imperial para a manutenção do habitat do planeta e, consequentemente, manutenção da vida humana.

c) respeito à capacidade de suporte dos ecossistemas. Nesses casos, é fundamental que se respeite os ciclos vitais da natureza e reduzindo o enfoque econômico,

conforme jjá se abordou acima. São necessárias alternativas às formas de produção atual, seja pela substituição ou mesmo pela redução na utilização desses recursos, trazendo a tona a ideia do decrescimento que pode ser uma via na minimização dos problemas socioambientais vez que o decrescimento é uma crítica radical ao modo de vida adotado pela sociedade moderna capitalista consumocentrista.

É importante, na presente fase deste artigo, que se aprofunde a ideia de decrescimento. O conceito econômico de decrescimento foi implementado na década de 70 pelo economista romeno Nicholas Georgescu-Roegen (2012), o qual entendia que havia a necessidade de se buscar alternativas para a sobrevivência da vida no planeta Terra, sendo que, para isso, evidenciava a relação entre a lei da entropia e os processos econômicos vigentes. Para o autor era preciso a busca efetiva de um desenvolvimento que fosse realizado de maneira sustentável, mas, para isso, haveria a necessidade de se criar uma economia que ficasse num estado estacionário, na qual a produção que excedesse a capacidade natural dos ecossistemas fosse detida. Seria dessa maneira que se conseguiria administrar o capital e o lucro e com isso se buscar a sustentabilidade.

Também Latouche, outro autor decrescentista, entende que tanto o sistema implantado na modernidade busca o lucro e a economia tem como fundamento o crescimento pelo âmbito unicamente econômica, sendo que não há uma preocupação com os recursos naturais e com a qualidade de vida para todos os cidadãos. Dessa maneira, existia a necessidade de se procurar uma alternativa de enfrentamento da situação que se instaura, por isso, o autor propôs três passos importantes: "Avaliar seu alcance (I), propor uma alternativa para o delírio da sociedade de crescimento, a utopia concreta do decrescimento (II), e, por fim, especificar os meios de sua realização (III)" (2009, p. XV). Com isso, "o decrescimento é um *slogan* político com implicações teóricas" (2009, p. 04). É preciso "enfatizar fortemente o abandono do objetivo do crescimento ilimitado, objetivo cujo motor não é outro senão a busca do lucro por parte dos detentores do capital, com consequências desastrosas para o meio ambiente e, portanto, para a humanidade" (2009, p. 04). Por estes parâmetros, "o decrescimento não é um crescimento negativo" (LATOUCHE, 2009, p.05), mas é uma maneira de reduzir a velocidade do crescimento que se impõe nas sociedades como uma forma de incerteza e de exclusão social, vez que, através dele ocorre o aumento da taxa de desemprego o abandono dos programas sociais, sanitários, educativos, ambientais e culturais que visam a garantia do mínimo vital, ou seja, do mínimo existencial às pessoas. (LATOUCHE, 2009, p.05). Com base nisso, os

problemas socioambientais do progresso e do desenvolvimento, feitos com base no lucro e consumo, poderiam ser minimizados.

Na América latina se utiliza a ideia do bem viver[16], inserida pelas constituições como, por exemplo, Equador (2008) como outra alternativa para a busca da sustentabilidade e da equidade social. Dessa maneira Martínez entende que a proposta da concepção de bem viver "provém de um sujeito histórico, cujos vínculos com a terra e a natureza não estão quebrados, mesmo apesar de todo o sofrimento histórico, do despojo e da destruição da natureza: os índios". Continua afirmando que "o bem viver, para eles, é mais do que viver melhor, ou viver bem: o bem viver é viver em plenitude. De fato, o termo utilizado não é "alli kawsay" (alli = bem; Kawsani = viver), mas sim "sumak Kawsay" (sumak = plenitude; kawsani = viver)". (MARTÍNEZ, 2010).

O Sumak Kawsay, inserido na Constituição equatoriana[17], se expressa em uma "relación diferente entre los seres humanos y con su entorno social y natural. El buen vivir incorpora una dimensión humana, ética y holística al relacionamiento de los seres humanos tanto con su propia historia cuanto com su naturaliza". (DÁVALOS, 2008, p.03). Para Wolkmer o bem viver seria a "redefinição de sociedade sustentável, erradicada de todas as formas produtivas de extrativismo e de visões mecanicistas de crescimento econômico, trazendo propostas inovadoras capazes de superar as ameaças globais à biodiversidade e de conscientizar a construção de uma sociedade que seja parte da natureza e que conviva harmonicamente com esta mesma natureza". (WOLKMER; WOLKMER, 2014, p.997).

Esse vínculo com a Terra permite que se respeitem os ciclos vitais da natureza, possibilitando que se possa viver melhor e viver na plenitude. O bem viver é uma forma de construir uma sociedade que tenha uma convivência que seja cidadã, conjuntamente

[16] Sumak Kawsay (buen vivir), que oferece vasta e substancial variedade de aportes, visto que "incorpora a la naturaleza en la história" e se traduz em um "cambio fundamental en la episteme moderna", herdeira do paradigma ocidental de dominação e objetificação da natureza. (DÁVALOS, 2008, p.3).

[17] O texto constitucional equatoriano denota em seu "Art. 1.- El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico. Se organiza en forma de república y se gobierna de manera descentralizada. La soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa previstas en la Constitución. Los recursos naturales no renovables del territorio del Estado pertenecen a su patrimonio inalienable, irrenunciable e imprescriptible". (ECUADOR, 2008).
Já no Título II, Segundo Capítulo, da Constituição Equatoriana, os "Derechos del Buen Vivir", se abordam questões diversificadas como, por exmplo: água, alimentação, ambiente saudável, comunicação e informação, cultura e ciência, educação, moradia, saúde, trabalho e seguridade social, juntamente com o Sumak Kawsay, que passa a estar presente nos diversos direitos que são garantidos constitucionalmente.

com o respeito à natureza. É uma nova racionalidade a ser construída, o que denota que existe a necessidade de mudança dos padrões individuais de consumo.

Voltando aos requisitos apontados por Araújo e acima elencados, no caso do requisito "e" - mudança dos padrões individuais de consumo e da alternativa – e "f" - que traz o fato de delinear ferramentas locais disponíveis –, pode-se trazer a democracia participativa e o fortalecimento dos espaços locais como formas de consolidar uma sustentabilidade socioecológica, visto que as pessoas conseguem mudar sua racionalidade e buscar uma nova conscientização e educação se houver o sentimento de pertencimento a esses espaços. Denis Rosenfield assevera que o "regime político democrático tem como objetivo alçar o indivíduo na informe vida cotidiana moderna, deste isolamento no qual vive, ao lugar da comunidade, ao lugar da solidariedade, onde o que é político pode ser visto e vivido por todos". (1994, p. 48).

Nalini entende que a sustentabilidade deve ser uma transformação social que "propõe a celebração da unidade homem/natureza, na origem e no destino comum e significa um novo paradigma. Não há necessidade de se renunciar ao progresso, para a preservação do patrimônio ambiental" (NALINI, 2001, p. 138).

Para Penna, a sustentabilidade é um processo de mudanças, portanto, existe a necessidade de se proteger a casa comum e para isso é essencial uma mudança de racionalidade, a qual permita que o ser humano possa ter uma visão ecocêntrica, ou seja, uma preocupação com os humanos e não humanos que habitam o planeta. Por isso segundo a doutrina social da Igreja Católica, na Encíclica Laudato Si, do Papa Francisco demonstra que "a cultura ecológica não se pode reduzir a uma série de respostas urgentes e parciais para os problemas que vão surgindo à volta da degradação ambiental, do esgotamento das reservas naturais e da poluição". Assim sendo "deveria ser um olhar diferente, um pensamento, uma política, um programa educativo, um estilo de vida e uma espiritualidade que oponham resistência ao avanço do paradigma tecnocrático. Caso contrário, até as melhores iniciativas ecologistas podem acabar bloqueadas na mesma lógica globalizada" (LAUDATO Si', 2015, §51). Com base no exposto acima é possível se buscar uma sustentabilidade, que seja socioecológica pautada na interligação ser humano com a natureza, visando a minimização dos impactos socioambientais causados pelo consumocentrismo, pelo progresso econômico na sociedade moderna.

Para se atingir a sustentabilidade socioecológica, é preciso uma visão sistêmica entre os seres humanos e a natureza. É importante salientar que, os problemas ambientais estão vinculados aos problemas sociais e vice-versa, sendo que ambos necessitam ser

resolvidos na sociedade moderna consumocentrista. O consumo como centro da sociedade não deve mascarar essas problemáticas, as pessoas devem buscar uma nova racionalidade, com a finalidade de se conscientizarem e se educarem, para rever o modo de consumo e de progresso existente na atualidade.

O antropocentrismo[18] e o consumocentrismo são dois problemas modernos, que precisam ser repensados e revistos na sociedade contemporânea, a fim de evitar os problemas socioambientais tão prementes e se atingir uma sustentabilidade, que pauta num viés socioecológico e que não seja usada como marketing mercadológico dessa sociedade.

3. Considerações finais

Com o exposto acima, se percebe que a sociedade consumocentrista é pautada com o consumo como centro da mesma, sendo isso um artifício da modernidade e do capitalismo a fim de adestrar e docilizar os sujeitos. Portanto, esses sujeitos acabam se imiscuindo em um vazio existencial, que leva a insatisfação e a desagregação social, sendo que os mesmos não percebem os problemas socioambientais que estão patentes nessa sociedade. É preciso se encontrar alternativas com a finalidade de minimizar esses problemas, sendo eles: a pobreza, o racismo, a desigualdade social, as mudanças climáticas, o racismo ambiental a poluição, etc.

O progresso e a modernidades associadas às tecnologias permitiram que a sociedade evoluísse, contudo, o ser humano acabou se tornando submisso a isso e deixando a alteridade de lado, para pensar somente em si. Essa alteridade não pode ser vista somente para os seres humanos, mas também, para os não humanos, ou seja, para a casa comum, é com isso que se consegue uma sustentabilidade socioecológica.

É importante se buscar a sustentabilidade, de forma plena e eficaz e não mercadologicamente, o mercado não pode transformá-la em uma bandeira de comércio e consumo, na qual as pessoas são iludidas a adquirirem bens por serem sustentáveis. A sustentabilidade deve ser uma interligação entre o ser humano e a natureza, onde deve haver o reconhecimento sistêmico da integração de ambos. A ideia da sustentabilidade

[18] Carvalho (1999, p.108) denota que "cabe negar o caráter sócio-antropocêntrico das ciências do homem, e seu imperialismo que pretende reificar o social, explicando, posivisticamente ou não, por suas próprias determinações. Se a cisão homem/natureza não faz mais sentido, uma vez que qualquer ser vivente é sempre auto-eco-organizador, o 'contrabando' de outros saberes será nucleado para a abertura da razão e a reforma do pensamento, a serem implementados por intelectuais mais polivalentes e menos 'proprietários' de seus objetos e saberes".

socioecológica se dá pelo fato de que se integre todos os sistemas sociais, políticos, culturais com os sistemas naturais, permitindo assim uma relação sistêmica entre todos.

A vida no planeta Terra necessita de uma mudança radical da racionalidade humana, a qual deve entender que não o ser humano não é o centro da natureza e, sim, é um ser que vive pela integração com os demais. Essa mudança permite que a conscientização do espaço do sujeito no Planeta possa ser avaliada e repensada e, assim é possível respeitar os ciclos vitais da natureza, aprofundando a ideia do bem viver e do decrescimento como alternativas para minimizar os impactos socioambientais causados na atualidade.

Os recursos naturais e seus ciclos vitais devem ser preservados para a continuidade da existência da humanidade e da natureza como a conhecemos. Importante, para que isso aconteça se ter em mente que os bens criados não sirvam para induzir o consumo de algo desnecessário e supérfluo, dentro de uma ideia de adestramento e docilização do sujeito, induzindo-o a necessidade dos mesmos para o alcance da felicidade. O consumocentrismo aliado ao antropocentrismo se mostra nefasto à sociedade moderna, e pode ser catalogado juntamente com os maiores erros que a humanidade já cometeu,

Pela análise efetuada no presente trabalho pode-se verificar o ser humano está intimamente – sistemicamente – ligado à natureza. Esta interligação demanda à proteção da natureza como elemento fundamental em si própria e, também, como possibilidade de sobrevivência da espécie humana. Dois aspectos essenciais foram levantados, o social e o ecológico, que sofrem com uma sociedade voltada para o consumo, assim: não se pode permitir que pessoas passem necessidades básicas, visto que a dignidade humana é um pressuposto universal; não se pode admitir que a natureza continue sendo destruída em nome de um progresso econômico excludente. Se as pessoas tiverem um *status* social adequado e sem desigualdade muitos problemas ambientais podem ser minimizados na atualidade. Não há como fechar os olhos para o que é evidente na sociedade contemporânea. O consumocentrismo pode adestrar os sujeitos para um mundo de fantasia, mas a realidade é outra – desigualdade e destruição ambiental – algo que está a nossa porta e precisa ser pensada. É a partir daí, que a conscientização vinda de uma nova racionalidade, conforme se abordou, permite que se possa ter uma sociedade melhor, mais justa e solidária e, com isso, o respeito aos ciclos vitais da natureza serão efetivados. É com base nesses aspectos que se pode buscar uma sustentabilidade que seja socioecológica.

4. Referências bibliográficas

ARAÚJO, Gisele Ferreira. **Estratégias de sustentabilidade.** São Paulo: Editora Letras Jurídicas, 2008. ISBN: 97-885-899-1738-4

BAUMAN, Zygmunt. **Modernidade e ambivalência.** Rio de janeiro: Jorge Zahar, 1999. **ISBN:** 97-885-711-0494-5.

CALGARO, Cleide. PEREIRA, Agostinho Oli Koppe. In **A sociedade consumocentrista e seus reflexos socioambientais: a cooperação social e a democracia participativa para a preservação ambiental.** 2016. Revista de Direito, Economia e Desenvolvimento Sustentável. Curitiba. v. 2. n. 2, p. 72 – 88. Jul/Dez. 2016. **ISSN**: 2526-0057

CARVALHO, Carlos Gomes de. **O que é Direito Ambiental**: dos descaminhos da casa à Harmonia da Nave. Florianópolis: Habitus, 2003. **ISBN**: 85-882-8318-2

CARVALHO, Edgard de Assis. *Complexidade e ética planetária.* In: PENA -VEGA, Alfredo; NASCIMENTO, Elimar Pinheiro do. O pensar complexo. 3. ed. Rio de Janeiro: Garamond, 1999. **ISBN:** 97-885-864-3525-6.

CAMPBELL, Colin; BARBOSA, Lívia (org). **Cultura, consumo e identidade**. Rio de Janeiro: FGV, 2007. **ISBN**: 85-225-0570-5

DÁVALOS, Pablo. **Reflexiones sobre el Sumak Kawsay (el buen vivir) y las teorias del desarrollo**. America Latina em Movimiento, 05 ago. 2008. p.3. Disponível em: http://alainet.org/active/25617&lang=es. Acesso em: 06 dezembro 2019.

DEBORD, Guy. **A sociedade espetáculo**. Trad. Estela dos santos Abreu. Rio de Janeiro: Contraponto, 1997. **ISBN**: 978-85-85910-4

ECUADOR. **Constitución del Ecuador de 2008**. Disponível em: <http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf>. Acesso em 02 dezembro 2019.

GIDDENS, Anthony. **As consequências da modernidade.** São Paulo: Unesp, 1991. **ISBN** 85-7139-022-3.

GUIMARÃES, Roberto P. **A ética da sustentabilidade e a formulação de políticas de desenvolvimento.** In: VIANA, Gilney; SILVA, Marina; DINIZ, Nilo. O desafio da

sustentabilidade: Um debate socioambiental no Brasil. São Paulo: Editora FundaçãoPerseuAbramo, 2001. p. 43- 71. **ISBN** 97-885-864-6946-6

GOFFMAN, Erving. **A representação do eu na vida cotidiana.** Trad. Maria Célia Santos Raposo. 20 ed. Petrópolis: Vozes, 2014. **ISBN**: 97-885-326-0875-8

GEORGESCU-ROEGEN, Nicholas. **O Decrescimento. Entropia, ecologia, economia.** Trad. Maria José Perillo Isaac. São Paulo: Senac, 2012. **ISBN**: 97-885-396-0269-8

HALL, Stuart. **A identidade cultural na pós-modernidade.** Tradução Tomaz Tadeu da Silva, Guaracira Lopes Louro. Rio de Janeiro: DP&A, 2004. **ISBN**: 8574903361

HARVEY, David. **Condição pós-moderna.** São Paulo: Edições Loyola, 18ª ed., 2009. **ISBN**: 97-885-150-0679-3.

HARVEY, David. **O novo imperialismo.** São Paulo: Edições Loyola, 2ª ed., 2005. **ISBN**: 97-885-150-2971-6.

LATOUCHE, Serge. **Pequeno tratado do decrescimento sereno.** São Paulo: Editora WMF, 2009. **ISBN**: 97-897-244-164-65.

LEFF, Enrique. **Saber ambiental**: sustentabilidade racionalidade, complexidade, poder. 2. ed. Rio de Janeiro: Vozes, 2002. **ISBN**: 85-326-2609-2.

LYON, David. **Pós-modernidade**. São Paulo: Paulus, 1998. ISBN: 85-349-1105-3.

LIPOVESTSKY, Gilles. **Os tempos hipermodernos**. São Paulo: Bacarolla, 2004. **ISBN**: 97-885-982-3305-5.

MARTÍNEZ, Esperanza. **Sumak kawsay.** Nem melhor, nem bem: viver em plenitude. Entrevista especial com Esperanza Martinez. Revista do Instituto Humanista Unisinos. 2010. [on line]. Disponível em: <http://www.ihu.unisinos.br/entrevistas/34622>. Acesso em 12 novembro de 2019. **ISSN**: 1981-8793.

MARTÍNEZ, Esperanza. **Pachamama y Sumak Kawsai.** 2012. Disponível em: <http:www.sicsal.net/reflexiones/CentenarioProanhoEMartinez.pdf>. Acesso em: 06 novembro 2019.

NALINI, José Renato. **Ética ambiental**. Campinas: Millennium, 2001. **ISBN**: 97-885-203-6313-3.

PAPA FRANCISCO. **Carta Encíclica Laudato Si' do Santo Papa Francisco sobre o Cuidado da Casa Comum**. 2015. Disponível em: <http://w2.vatican.va/content/francesco/pt/encyclicals/documents/papa-francesco_20150524_enciclica-laudato-si.html>. Acesso em: 29 dezembro 2019.

PEREIRA, Agostinho Oli Koppe; PEREIRA, Henrique Mioranza Koppe. **A modernidade e a questão da vida**. In: PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide. Direito Ambiental e Biodireito: da modernidade à pós-modernidade. Caxias do Sul: EDUCS, 2008. **ISBN**: 97-885-706-1489-6.

PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide. **A modernidade e o hiperconsumismo: políticas públicas para um consumo ambientalmente sustentável**. In: PEREIRA, Agostinho Oli Koppe; HORN, Luiz Fernando Del Rio (Orgs.). *Relações de consumo*: políticas públicas. Caxias do Sul, RS: Plenum, 2015. **ISBN**: 97-885-885-1264-1.

PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide. **Os riscos ambientais advindos dos resíduos sólidos e o hiperconsumo**: a minimização dos impactos ambientais através das políticas públicas. In: PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide; HORN, Luiz Fernando Del Rio (Orgs.). *Resíduos sólidos*: consumo, sustentabilidade e riscos ambientais. Caxias do Sul, RS: Plenum, 2014. **ISBN**: 97-885-885-1263-4.

PEREIRA, Agostinho Oli Koppe; LUNDGREN, Ana Paula; TONIASSO, Rachel Cassini. **O hiperconsumo e os riscos ambientais provocados por resíduos sólidos**: uma análise da política nacional dos resíduos sólidos, tendo Caxias do Sul como referência. In: PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide; HORN, Luiz Fernando Del Rio (Orgs.). *Hiperconsumo, riscos ambientais*: provocados pelos resíduos sólidos e políticas públicas nos municípios de Caxias do Sul e Passo Fundo. Caxias do Sul, RS: Plenum, 2014. **ISBN**: 97-885-885-1262-7.

PEREIRA, Agostinho Oli Koppe; CALGARO, Cleide; PEREIRA, Henrique Mioranza Koppe. **Consumocentrismo e os seus reflexos socioambientais na sociedade contemporânea**. *Revista Direito Ambiental e Sociedade*, v. 6, p. 264-279, 2016. **ISSN**: 2316-8218.

PEREIRA, Agostinho Oli Koppe; SIMIONI, Rafael Lazzarotto. Da maximização à eficiência: o sentido de consumo na semântica econômica moderna. PEREIRA, Agostinho Oli Koppe; HORN, Luiz Fernando del Rio (Org.). **Relações de Consumo**: Consumismo. Caxias do Sul: Educs, 2010. **ISBN**: 97-885-706-1563-3.

PEREIRA, Agostinho Oli Koppe. CALGARO, Cleide. **Impacto ambiental do hiperconsumo na sociedade moderna**: as políticas públicas de sustentabilidade local. Revista Jurídica, Curitiba, v. 3, n. 44, p. 232-256. 2016. **ISSN**: 2316-753X.

PENNA, Carlos Gabaglia. **O estado do planeta.** A sociedade de consumo e degradação ambiental. Rio de Janeiro: Record, 1999. **ISBN**:978850105686-3

ROSENFIELD, Denis Lerrer. **O que é democracia**. 5.ed. São Paulo: Brasiliense, 1994. **ISBN**-10: 8511012192; **ISBN**-13: 978-8511012194

SACHS, Ignacy. **Desenvolvimento includente, sustentável, sustentado**. Rio de Janeiro: Garamond, 2004. **ISBN**-10: 857617040X; **ISBN**-13: 978-8576170402

SCHNEIDER, Peter. "**O fetichismo do consumo**". In: PIETROCOLA, L.G. (Org.) *O Que Todo Cidadão Precisa Saber Sobre Sociedade de Consumo*. São Paulo: Global. Caderno de Educação Política, Série: Sociedade e Estado (18), 1986. **ISBN**: 20-000-655-0900-3.

SOLOMON, M. **O Comportamento do consumidor comprando, possuindo e sendo**. 5ª ed. São Paulo: Bookman. 2002. **ISBN**: 85-826-0367-3.

WOLKMER, Antônio Carlos. **Pluralismo e Crítica do Constitucionalismo na América Latina**. In.: Anais do IX Simpósio Nacional de Direito Constitucional. Anais eletrônicos, 2011, p. 151. Disponível em <http://www.abdconst.com.br/revista3/antoniowolkmer.pdf>. Acesso em 06 ago 2018. **ISBN**: 978-85-65693-00-4

_____. **Pluralismo Jurídico**: fundamentos de uma nova cultura no Direito. 3º ed. São Paulo: Alfa-Omega, 2001. **ISBN**: 85-022-2835-8.

_____; WOLKMER, Maria de Fátima S. **Repensando a Natureza e o Meio Ambiente na Teoria Constitucional da América Latina**. In.: Revista Novos Estudos Jurídicos, Nº 3, Vol. 19, Set-Dez. 2014. Disponível em: < http://www6.univali.br/seer/index.php/nej/article/view/6676>. Acesso em 31 jul 2018. **ISSN**: 2175-0491.

Decisões Automatizadas e Processos Discriminatório: a Lei Geral de Proteção de Dados brasileira como mecanismo de governança

Núbia Franco de Oliveira[19]
Deilton Ribeiro Brasil[20]
Jamile Bergamaschine Mata Diz[21]

RESUMO

Em que pesem os inúmeros benefícios decorrentes do recente desenvolvimento de tecnologias de inteligência artificial, diversos desafios socioeconômicos, éticos e jurídicos se afiguram. O presente artigo visa demonstrar como algoritmos, embora sejam pretensamente neutros, podem ser enviesados, passando a produzir resultados discriminatórios e danosos à sociedade. Este problema toma proporções maiores a partir do crescimento da utilização de decisões automatizadas que são, majoritariamente, opacas quanto ao seu modo de funcionamento. Visa-se demonstrar como a regulamentação legal acerca da proteção de dados pessoais serve como mecanismo de governança capaz de mitigar prejuízos causados por decisões automatizadas, notadamente a Lei Geral de Proteção de Dados (Lei nº 13709/2018). As metodologias adotadas foram a dedutiva e a crítico-dialética. Dedutiva porque, a partir de certas premissas, serão construídas conclusões sobre a temática apresentada, respeitando-se uma estrutura lógica de pensamento. Crítico-dialética, porque a exposição estimula o diálogo teórico e a reflexão acerca do tema proposto, com a abordagem de categorias consideradas fundamentais para o desenvolvimento da presente investigação.

PALAVRAS-CHAVE

Decisões automatizadas; Enviesamento algorítmico; LGPD; Governança.

[19] Mestranda do PPGD – Mestrado e Doutorado em Proteção dos Direitos Fundamentais da Universidade de Itaúna (UIT). Graduada em Direito pela Universidade Federal de Juiz de Fora-UFJF. Pós-graduada em Direito Processual Civil pela Instituição de Ensino Damásio Educacional.
[20] Pós-Doutor em Direito pela UNIME, Itália. Doutor em Direito pela UGF-RJ. Professor da Graduação e do PPGD - Mestrado e Doutorado em Proteção dos Direitos Fundamentais da Universidade de Itaúna (UIT), Faculdades Santo Agostinho (FASASETE-AFYA), Faculdade de Direito de Conselheiro Lafaiete (FDCL). Professor visitante da Universidade de Caxias do Sul (UCS).
[21] Coordenadora do Centro de Excelência Europeu Jean Monnet UFMG. Cátedra Jean Monnet Direito UFMG. Professora Faculdade de Direito da Universidade Federal de Minas Gerais (UFMG). Professora da Universidade de Itaúna. Professora da ESDHC e da FDMC/MG. Doutora em Direito Público/Direito Comunitário pela Universidad Alcalá de Henares - Madrid. Mestre em Direito pela UAH, Madrid Master en Instituciones y Políticas de la UE - UCJC/Madrid.

Automated Decisions and Discriminatory Processes; the Brazilian General Data Protection Law as a governance

ABSTRACT

In spite of the countless benefits resulting from the recent development of artificial intelligence technologies, several socioeconomic, ethical and legal challenges appear. This article aims to demonstrate how algorithms, although supposedly neutral, can be biased, starting to produce discriminatory and harmful results to society. This problem takes on greater proportions due to the growth in the use of automated decisions, which are mostly opaque in terms of their way of functioning. It aims to demonstrate how the legal regulation on the protection of personal data serves as a governance mechanism capable of mitigating losses caused by automated decisions, notably the General Data Protection Law (Law No. 13.709 of 2018). The methodologies adopted were deductive and critical-dialectic. Deductive because, based on certain premises, conclusions that will be built on the presented theme, respecting a logical structure of thought. Critical-dialectic, because the exhibition stimulates theoretical dialogue and reflection on the proposed theme, with the approach of categories considered fundamental for the development of the present research.

KEYWORDS

Automated decisions; Algorithmic bias; LGPD; Governance.

Introdução

Nos últimos anos, a expressão "inteligência artificial" (IA) passou a ocupar a maioria dos âmbitos do cotidiano. Desde o uso de *smartphones* e redes sociais, passando pelas novas relações de consumo, chegando às áreas da saúde e da segurança pública, novas tecnologias têm adquirido relevância e, com isso, ubiquidade, fazendo-se cada vez mais presentes nas vidas das pessoas. A questão é que, em que pesem os inúmeros benefícios decorrentes do recente desenvolvimento de tecnologias de inteligência artificial, diversos desafios socioeconômicos, jurídicos e sobretudo éticos decorrem da sua utilização.

Um dos principais desafios está relacionado àquilo que se denomina "enviesamento" dos algoritmos: por vezes, mesmo "máquinas inteligentes", dotadas de IA, reproduzem vieses ou preconcepções de seus programadores, o que acaba por refletir em resultados negativos obtidos a partir do seu emprego. Isso ocorre, como se demonstrará adiante, em razão de uma série de fatores, como bases de dados enviesadas ou a falta de diversidade na equipe de engenheiros e *designers* responsáveis pelo desenvolvimento das tecnologias.

Diante desse cenário, é necessário compreender em que medida se pode coibir os danos causados pelo enviesamento algorítmico em decisões automatizadas através da utilização da regulamentação legal como mecanismo de governança. Existem, evidentemente, diversas abordagens a serem adotadas, e é justamente nesse sentido que o presente trabalho coloca a seguinte hipótese: em que medida os limites legais podem servir como salvaguarda dos direitos dos titulares no que se refere à tomada de decisões automatizadas?

Para tanto, dividiu-se a pesquisa em dois momentos distintos. Primeiramente, faz-se uma análise sobre os atuais usos das tecnologias de inteligência artificial, destacando casos emblemáticos de discriminações e enviesamento dessas tecnologias. Em seguida, dar-se-á enfoque na utilização de decisões automatizadas e no modo como a legislação vigente, notadamente a LGPD e o RGPD, servem como base para regulamentar o uso desta tecnologia e, consequentemente, dirimir danos que dela poderão advir.

A pesquisa procura compreender como legislações como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados da União Europeia (RGPD) seriam capazes de fornecer parâmetros aptos a mitigar e/ou prevenir eventuais discriminações advindas do uso de inteligência artificial no tratamento de dados em processos decisórios automatizados. As metodologias adotadas foram a dedutiva e a

crítico-dialética. Dedutiva porque, a partir de certas premissas, serão construídas conclusões sobre a temática apresentada, respeitando-se uma estrutura lógica de pensamento. Ademais, parte-se de uma compreensão geral sobre o assunto para adentrar-se o contexto específico da realidade brasileira. Crítico-dialética, porque a exposição estimula o diálogo teórico e a reflexão acerca do tema proposto, com a abordagem de categorias consideradas fundamentais para o desenvolvimento da presente pesquisa.

Os procedimentos técnicos utilizados na pesquisa para coleta de dados foram essencialmente a pesquisa bibliográfica e documental. O levantamento bibliográfico forneceu as bases teóricas e doutrinárias a partir de livros e textos de autores de referência, tanto nacionais como estrangeiros. Enquanto o enquadramento bibliográfico utiliza-se da fundamentação dos autores sobre um assunto; o documental articula materiais que não receberam ainda um devido tratamento analítico. A fonte primeira da pesquisa é documental e bibliográfica (que instruiu a análise da legislação constitucional e a infraconstitucional, bem como a doutrina que informa os conceitos de ordem dogmática).

1. Discriminação algorítmica: do enviesamento das bases de dados ao emprego de tecnologias discriminatórias

A maioria das pessoas tende a crer que os sistemas baseados em inteligência artificial são, por natureza, neutros, objetivos e imparciais, o que faz com que cada vez mais confiança seja depositada em algoritmos, que realizam tomadas de decisões que podem influenciar a vida cotidiana de cada um de nós. Por vezes, tais decisões são irrelevantes ou supérfluas, como a recomendação de um filme em alguma plataforma de *streaming* ou a sugestão de um produto em um *site* de vendas. Por outras, podem se referir a questões verdadeiramente importantes, como a concessão de um empréstimo, a possibilidade de financiamento de um imóvel ou, até mesmo, o período de detenção que determinada pessoa deverá cumprir em razão do cometimento de um crime. Um dos motivos que leva à confiança nesses sistemas inteligentes é justamente a crença na sua objetividade: uma vez que as decisões são tomadas a partir da análise de dados, a subjetividade humana é supostamente neutralizada e resultados mais justos e imparciais são obtidos. Contudo,

> tal presunção não se mostra verídica, uma vez que esses sistemas podem refletir os preconceitos e vieses humanos já existentes na sociedade, de forma a violar direitos humanos variados, especialmente de grupos historicamente marginalizados , como negros, mulheres, deficientes, pobres, membros da comunidade LGBT e até alguns grupos étnicos minoritários. (GUEDES, 2020, p. 1)

Segundo Ruha Benjamim, "a tecnologia não é apenas uma metáfora racial, mas um dos muitos meios pelos quais as formas anteriores de desigualdade são atualizadas" (2020, p. 17). Isso significa dizer que, ainda que novas tecnologias não sejam *responsáveis* pelo surgimento de tratamentos discriminatórios, como racismo ou sexismo, elas correspondem a meios de reprodução e perpetuação dessas formas de violência. Dessa forma, é imprescindível que, no estudo dos valores, suposições e manifestações de vontade que perpassam as inovações científicas e tecnológicas, os pesquisadores estejam atentos às diferentes formas de tratamento que podem se manifestar no *design* da tecnociência (BENJAMIM, 2020).

Essas manifestações, às quais nos referiremos como "enviesamento algorítmico", decorrem de uma série de fatores, como aponta Tarcízio Silva (2020). Primeiramente, devemos ter em mente que atos atentatórios e discriminatórios, como o racismo, decorrem de um "sistema sociopolítico global que inclui historicamente formatações dos campos produtivos da tecnologia que favorecem o treinamento enviesado de sistemas que intensificam discriminações e opressões" (SILVA, 2020, p. 124). Além disso, como os algoritmos são desenvolvidos por pessoas, é inevitável que essas pessoas - especialmente os programadores – incorporem seus próprios vieses, geralmente inconscientes, nesses algoritmos (SILVA, 2020). Em outras palavras,

> Hoje, não há mais dúvidas de que a IA, como tecnologia emergente, possui enorme capacidade de reproduzir, reforçar e até exacerbar a desigualdade já existente em diferentes contextos, já que a tecnologia é produto da sociedade, de seus valores, prioridades e, inclusive, desigualdades, o que inclui as relacionadas ao racismo, ódio e intolerância. O design e o uso dessas ferramentas podem, direta ou indiretamente, de forma intencional ou não, discriminar determinados grupos sociais. Muitas dessas possíveis violações de direitos humanos não são novas, mas exacerbadas pela escala, volume, rápida (e descuidada) proliferação e impactos reais imediatos facilitados pela IA. A marginalização e discriminação de certas camadas da sociedade são, então, refletidas nos dados e reproduzidas nos resultados que consolidam padrões históricos de preconceitos enraizados. (GUEDES, 2020, p. 1)

A fim de ilustrar como o enviesamento algoritmo pode afetar comunidades específicas, Benjamim (2020) cita um relatório recente sobre "viés de máquina", no qual pesquisadores foram capazes de ilustrar como ferramentas de avaliação de riscos geradas por computador são tendenciosas contra americanos negros. A fórmula empregada pelo sistema de auxílio à tomada de decisões judiciais sinalizava falsamente que réus negros eram mais propensos à reincidência criminal, indicando que as chances de voltarem a cometer algum crime eram duas vezes maiores quando comparados com réus brancos, e

que, além disso, eram mais propensos ao cometimento de crimes violentos (ANGWIN et al., 2016). Essa diferenciação, aponta Paula Guedes, "ocorre principalmente em razão da utilização de dados históricos de prisões e condenações anteriores, que acabam por perpetuar práticas policiais e judiciais racistas, exacerbando as disparidades raciais enraizadas na sociedade" (GUEDES, 2020, p. 2).

A questão é que "essa 'discriminação algorítmica' não se limita ao trabalho policial; os tentáculos sufocantes do Estado carcerário abrangem escolas, hospitais e outras instituições que buscam controlar pessoas pobres e racializadas" (BENJAMIM, 2020, p.17). Isso se dá porque, ainda que os sistemas dotados de inteligência artificial não utilizem o critério racial enquanto critério de análise, determinados padrões sociais para a avaliação de risco, como nível de escolaridade, taxa de emprego ou análise de antecedentes criminais podem resultar em discriminação racial indireta (GUEDES, 2020). A desigualdade socioeconômica, reflexo do racismo estrutural presente em algumas sociedades, faz com que mesmo sistemas supostamente objetivos, em razão da utilização de algoritmos, reproduzam padrões de opressão e discriminação, fazendo com que determinadas pessoas sejam privadas de determinados bens ou serviços e até mesmo tenham seus direitos fundamentais violados em decorrência da suposta "objetividade" algorítmica.

Na realidade, infelizmente, exemplos da forma como as inteligências artificiais reproduzem vieses e preconceitos humanos não são raros, tampouco se atêm a situações ligadas à atuação estatal. À medida que novas tecnologias ganham espaço no cotidiano, mais se percebe, tanto em assuntos considerados como de mínima intervenção, quanto em assuntos vitais, como as inovações tecnológicas são imbuídas de vieses discriminatórios. Um caso curioso é o de uma mulher coreana que teve seu cabelo aspirado por um robô-aspirador: o aparelho, que tem se tornado cada vez mais comuns em residências, consiste de um aspirador de pó em formato de disco, que realiza a limpeza de superfícies sem a necessidade de controle humano. Para isso, geralmente conta com sensores que detectam a presença de sujeiras no chão e realizam a aspiração. Ocorre que, no desenvolvimento do produto, não foi levado em consideração que é comum que em alguns países as pessoas durmam ou descansem no chão. Assim, o robô confundiu o cabelo da mulher com sujeira e o aspirou, de modo que ela teve de contar com o auxílio de uma equipe médica para "soltá-la" (MCCURRY, 2015).

Pode-se apontar ainda o uso de ferramentas de detecção de rostos em câmeras fotográficas. Em 2009, a Nikon, uma das maiores fabricantes desses aparelhos no mundo,

anunciou uma funcionalidade que permitia excluir automaticamente fotos em que o sujeito fotografado estivesse com os olhos fechados. Embora a intenção fosse facilitar o uso dos aparelhos pelos usuários, indicando quando fosse necessário tirar uma nova fotografia, a ferramenta, na maioria das vezes, era incapaz de detectar que pessoas asiáticas estavam com os olhos abertos, excluindo indevidamente suas fotos (ROSE, 2010). Outro caso que ganhou notoriedade é o do algoritmo de classificação de fotos da *Google*, que confundiu pessoas negras com chimpanzés ou gorilas. Duramente criticado, o sistema de IA foi "corrigido" mediante a exclusão dos animais do léxico do aplicativo para gestão de fotos pessoais; assim, em vez de "treinar" o algoritmo para que não confundisse seres humanos com símios ou outros macacos, a resposta da empresa se deu no sentido de apenas impedir a comparação (SALAS, 2018).

Sistemas de reconhecimento facial são particularmente preocupantes quando seu uso se dá para fins de segurança pública ou vigilância. De acordo com uma pesquisa realizada pelo NIST[22], órgão de pesquisa do governo dos Estados Unidos da América, os algoritmos de reconhecimento facial disponíveis no país chegam a apresentar índices de "falso positivo" (quando o sistema erroneamente identifica uma pessoa como sendo outra) para asiáticos e afro-americanos até 100 vezes mais altos do que para brancos; além disso, alguns dos algoritmos apresentavam maior dificuldade de reconhecer o gênero de mulheres negras, apontando-as como homens, e não mulheres, em até 35% das vezes (AFP, 2019). Destarte, sistemas de reconhecimento facial não representam apenas uma ameaça ao direito à privacidade, mas também à liberdade e à igualdade, exacerbando discriminações contra determinadas comunidades e indivíduos historicamente oprimidos (NEGRI; OLIVEIRA; COSTA, 2020).

Outra questão preocupante está ligada à reprodução de vieses discriminatórios em plataformas de buscas e redes sociais. O *Facebook*, por exemplo, diminuiu o alcance e "escondeu" publicações de manifestações contra violência policial racista, ao passo que o Twitter decidiu não banir discurso de ódio nazista/supremacista branco para não afetar políticos republicanos estadunidenses (SILVA, 2020). Além disso, o sistema de anúncios e publicidade do Google permite que empresas exibam anúncios sobre crimes direcionados especificamente a afro-americanos, e resultados de pesquisas na ferramenta de busca de imagens apresentam hipersexualização de garotas e mulheres negras.

[22] NIST é o acrônimo de *National Institute of Standards and Technology* (em tradução livre, Instituto Nacional de Padrões e Tecnologia).

Especificamente em relação a buscas em banco de imagens, Fernanda Carrera realizou um estudo nos principais bancos de imagens digitais[23] do mercado, constatando que estes são "vetores fundamentais para a manutenção do racismo estrutural, uma vez que (...) associam indivíduos negros a determinados contextos de emprego e renda que não se igualam aos contextos associados a indivíduos brancos" (CARRERA, 2020, p. 145). A título ilustrativo, a pesquisa pela palavra "*boss*" (chefe, em inglês) traz como resultado majoritariamente imagens de homens brancos; imagens com mulheres representando cargos de chefia correspondem a aproximadamente 28% dos resultados, enquanto homens negros e mulheres negras são representados em cargos de liderança em aproximadamente 3% e 2% dos resultados, respectivamente. Em contrapartida, a palavra "*secretary*" (que significa secretário ou secretária, sem marcação de gênero) leva a resultados que retratam sobretudo mulheres, muitas delas negras. Em mais um exemplo analisado na pesquisa, constatou-se que a palavra "*poverty*" (pobreza, em inglês) está relacionado principalmente a pessoas negras, com expressivo aumento de pessoas indígenas, mulheres e crianças; quando se busca a palavra "riqueza", por sua vez, "ao contrário dos resultados para pobreza, a branquitude reina como maioria na riqueza, assim como há aumento expressivo da presença de homens, sobretudo sozinhos" (CARRERA, 2020, p. 151).

Resultados semelhantes são obtidos quando o processo realizado é o inverso, isto é, quando se utilizam *softwares* de reconhecimento de objetos e imagens, em vez da busca de imagens a parir de palavras-chave. Em um estudo realizado com cinco dos principais algoritmos de reconhecimento de objetos disponíveis atualmente, foram analisados objetos "comuns", existentes em lares de diferentes países, os quais foram divididos por critérios de renda média mensal. Os pesquisadores descobriram que os algoritmos de reconhecimento de objetos cometeram cerca de 10% mais erros quando solicitados a identificar itens de uma residência com uma renda mensal de 50 dólares, em comparação com aqueles de uma residência que ganhava mais de 3.500 dólares; a diferença absoluta na precisão foi ainda maior, uma vez que os algoritmos foram de 15% a 20% melhores na identificação de itens dos EUA em comparação com itens de países como Somália e

[23] "Os bancos de imagens digitais, representados aqui pelo *Shutterstock*, *Stockphotos* e *Getty Images*, são repositórios de fotografias, ilustrações e vetores para fins comerciais e de circulação pública ou privada. Uma das principais fontes de imagem do mercado publicitário e editorial, estes bancos são uma ferramenta menos dispendiosa do que a produção independente e exclusiva de imagens para ilustração da peça discursiva. Por meio de busca de palavras-chave e alguns filtros e categorias, é possível encontrar e pagar pelo uso de imagens adequadas a qualquer intencionalidade criativa de produção, uma vez que, em geral, cada busca gera dezenas de páginas e milhares de resultados "relevantes"." (CARRERA, 2020, p. 139)

Burkina Faso (VINCENT, 2019). Os autores do estudo apontaram ainda que esse tipo de erro é comum quando se trata da análise de imagens de eventos, *e.g.*, casamentos, que possuem simbologias e elementos visuais distintos em diferentes culturas (VINCENT, 2019).

De maneira geral e independentemente do sistema de IA a que nos refiramos, esses erros e "confusões" decorrem de três principais fatores. O primeiro deles é a falta de precisão, ou acurácia, dos sistemas – em outras palavras, de limitações técnicas dos programas que impedem que apresentem resultados 100% eficazes. O segundo está relacionado às bases de dados que alimentam os sistemas: a maioria dos algoritmos de inteligência artificial são "treinados" (aprimorados) a partir de dados inseridos pelos programadores, como informações econômicas, estatísticas, imagens, *etc*.

Ocorre que, frequentemente, a base de dados por si só é enviesada, por exemplo, contando majoritariamente com imagens de pessoas brancas, o que faz com que os resultados obtidos a partir da aplicação do sistema reflitam esse enviesamento. Por fim, o terceiro fator – que está, de certa forma, relacionado ao segundo – refere-se à falta de diversidade dos programadores. Como vimos anteriormente, as IAs são criadas por seres humanos que, involuntariamente, inserem vieses cognitivos e sociais na criação desses sistemas. Uma vez que esses programadores são, em sua maioria, homens brancos, é comum que os algoritmos por eles criados deixem de levar em consideração aspectos relacionados a gênero, cor da pele e, também, questões culturais e étnicas.

Considerando que sistemas de inteligência artificial têm se mostrado cada vez mais presentes em nosso cotidiano, revela-se imprescindível pensar modos de mitigar resultados indesejados, sobretudo quando da utilização de decisões automatizadas que, por se fazerem cada vez mais presentes na sociedade digital, poderão potencializar ainda mais os danos causados por algoritmos enviesados.

2. Decisões automatizadas e a regulamentação como mecanismo de governança

2.1 O conceito e os impactos das decisões automatizadas

Como visto, ilusoriamente pode-se acreditar que algoritmos geridos por IA são capazes de propiciar resultados mais satisfatórios e otimizados que processos geridos por pessoa

humana, devido à utilização de técnicas como *machine learning* [24] ou *deep learning*[25]. Tarleton Gillespie (2014) salienta que, de fato, os algoritmos são inertes e que não possuem um sentido autônomo enquanto não estiverem ligados a bases de dados sobre as quais venham a funcionar. No entanto, sistemas de inteligência artificial comumente reproduzem formas de violência ocasionadas pelo treinamento enviesado de algoritmos e, consequentemente, geram prejuízos individuais e coletivos que podem incidir tanto na esfera pública quanto na privada.

Quando se pensa em sistemas dotados de inteligência artificial, devemos levar em conta que, assim como acontece com os seres humanos, ser inteligente não significa ser desprovido de vieses e preconceitos (BARSS, 2019). Máquinas inteligentes "aprendem" sobre o mundo a partir dos comandos humanos que, por sua vez, refletem suas perspectivas históricas, linguísticas e culturais, o que significa dizer que os sistemas de IA podem absorver tanto as características positivas quanto as negativas das pessoas.

E é precisamente através da utilização de sistemas avançados de IA que são concebidas as decisões automatizadas. Estas, por sua vez, podem ser entendidas como fruto do tratamento de dados realizado exclusivamente por mecanismos de inteligência artificial, ou seja, são decisões tomadas sem a participação humana. Destaca-se que a atividade humana na alimentação do sistema com dados ou na realização de interpretação de resultados apresentados pelo *software* não excluem o caráter automatizado da decisão (FERRARI, BECKER, 2021).

É relevante salientar que nem o RGPD e nem a LGPD definem de forma clara o que é uma decisão automatizada. Além disso, os diplomas legais supracitados não precisam sobre quais tipos de decisão automatizada podem afetar direitos juridicamente tutelados pelos titulares dos dados, tampouco qual é o grau de transparência e explicação de que deverão ser dotadas (FRAZÃO, 2018a).

No âmbito do RGPD Axel von dem Bussche e Paul Voigt (2017) asseveram que a mera participação de pessoal natural no processo decisório não descaracteriza seu caráter automatizado: é preciso que esta participação seja significativa ao ponto de ser

[24] *Machine leraning* ou *"*aprendizado de máquina é uma área de IA cujo objetivo é o desenvolvimento de técnicas computacionais sobre o aprendizado bem como a construção de sistemas capazes de adquirir conhecimento de forma automática. Um sistema de aprendizado é um programa de computador que toma decisões baseado em experiências acumuladas através da solução bem-sucedida de problemas anteriores." (MONARD, BARANAUSKAS 2003. p. 89)

[25] *Deep Learning* ou aprendizagem profunda é uma divisão da Aprendizagem de Máquina que pesquisa técnicas para simular o comportamento do cérebro humano em tarefas como reconhecimento visual, reconhecimento de fala e processamento de linguagem natural (FERNANDES, SILVA, 2018).

capaz de retroceder a deliberação automatizada. No entanto, ainda assim, torna-se uma tarefa complexa determinar, em casos concretos, qual será o grau necessário de intervenção de pessoa humana no processo decisório capaz de afastar a aplicação dos direitos de revisão, explicação e oposição previstos, tanto na LGPD como no RGPD (FRAZÃO, 2018a).

A discussão sobre o modo como são utilizadas e regulamentadas as decisões automatizadas efervescem à medida em que estas passam a integrar cada vez mais o tecido social. As decisões desta espécie abrangem desde situações teoricamente mais inofensivas, como o direcionamento personalizado de anúncios publicitários até a formação de métodos que captam o perfil completo de pessoas e atribuem a elas *scores* que, comumente, são utilizados para sistemas de proteção de crédito, afetando a vida financeira destas pessoas (HILDEBRANDT, 2019).

Tendo em vista o problema que se afigura, torna-se evidente a necessidade de projetar mecanismos que mitiguem os danos causados pelo emprego de processos tecnológicos que envolvam decisões automatizadas. A resposta para esta demanda encontra arcabouço na regulamentação legal como instrumento de governança, como veremos a seguir.

2.2 LGPD: um novo marco normativo na legislação brasileira

O advento de recentes avanços tecnológicos provocou a identificação dos dados pessoais com aspectos intrínsecos da personalidade. O direito à proteção de dados pessoais, assim, passou a figurar como direito indispensável à concretização da dignidade humana (MULHOLLAND, 2018). Desta forma, a instituição de um regime jurídico autônomo para a proteção de dados pessoais tornou-se imprescindível. Assim, despontou como resposta às demandas narradas a Lei Geral de Proteção de Dados brasileira, Lei nº 13.709/2018, fortemente inspirada no Regulamento Geral sobre a Proteção de Dados (RGPD) adotada pela União Europeia[26]. Nesse sentindo, Monteiro explica que a LGPD

> Foi inspirada nas discussões que culminaram na RGPD europeia e tem por objetivo não apenas conferir às pessoas maior controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. Isso inclui modelos de negócio que se valem de algoritmos para auxiliar na tomada de decisões automatizadas. A LGPD também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos nesse processo, por meio da diminuição da assimetria de

[26] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

> informações, e, por consequência, de poder, entre o indivíduo, setor privado e o Estado. (MONTEIRO, 2018)

Destaca-se que a LGPD se configura como um marco legislativo de natureza extremamente técnica, visto que agrupou mecanismos de controle cuja finalidade é assegurar que as garantias nela designadas sejam cumpridas, objetivando a proteção dos direitos humanos (PINHEIRO, 2020). Possuindo também natureza principiológica já que a Lei brasileira em seu art. 6º[27] prescreve uma série de princípios que deverão ser observados, para que sejam minoradas as possibilidades de ocorrência de decisões automatizadas com viés discriminatório e dotadas de opacidade.

A informação passou a ser elemento nuclear para o desenvolvimento humano, configurando nova forma de organização social, sedimentada pela evolução tecnológica e que criou mecanismos capazes de processar e transmitir informações de modo cada vez mais veloz (BIONI, 2018). Considerando este contexto, a LGPD objetivou, segundo Monteiro (2018), fornecer às pessoas gerência mais aguçada sobre seus dados pessoais, ao mesmo tempo em que visa propiciar substrato capaz de impulsionar o desenvolvimento econômico e tecnológico de forma adequada.

A LGPD desponta-se como marco regulatório no Brasil ao harmonizar um ecossistema que abrangia mais de quarenta normas setoriais que regulam a proteção de

[27] LGPD. Artigo 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

dados pessoais e a privacidade (MONTEIRO, 2018). Por essa razão, tornou o arcabouço legal brasileiro juridicamente mais estável e completo, uma vez que, ao sobrepor regulações normativas pré-existentes, eliminou uma série de contradições e lacunas. Destarte, o supracitado diploma legal passou a ser "um freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas" (FRAZÃO, 2019, p. 103).

2.2.1 Tratamento legal das decisões automatizadas

A Lei Geral de Proteção de Dados, em seu art.20, prevê que o titular dos dados tem direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e ainda que o controlador dos dados deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada (BRASIL, 2018). O objetivo da norma citada é fornecer parâmetros legais capazes de inibir o potencial lesivo de que são dotadas as decisões automatizadas. A justificativa reside no fato de que a utilização de algoritmos baseados em inteligência artificial torna estas decisões obscuras e, "sem a devida transparência, é muito provável que a programação possa estar permeada de vieses e preconceitos dos programadores, intencionais ou não." (FRAZÃO, 2019)

O potencial lesivo de decisões automatizadas pode ser percebido ao analisarmos o cuidado trazido pelo RGPD que, em seu art. 22, apregoa que o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, excetuando-se as situações excepcionalmente previstas (UNIÃO EUROPEIA, 2016). Neste mesmo sentido, Frazão (2019) explica que o direito de não ser sujeito a uma decisão totalmente automatizada deve ser respeitado, notadamente em casos em que esta tenha efeitos jurídicos ou significativos sobre a vida dos indivíduos.

A legislação brasileira, por outro lado, deixa de estabelecer iguais restrições às decisões automatizadas. Interessa destacar que o art. 20 da LGPD passou por alterações legislativas culminadas pela instituição da Lei 13.853/2019, a qual, além de instituir a Autoridade Nacional de Proteção de Dados (ANPD) brasileira, alterou a redação de determinados dispositivos do texto original da lei. O direito que o titular de dados (até então) possuía de solicitar a revisão *por pessoa natural* de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais foi retirado, de modo que, com

a nova redação, garante-se o direito à revisão, mas esta poderá ser realizada também mediante o emprego de algoritmos. Diante dessa alteração, a Coalização Direitos na Rede[28], manifestou-se contrariamente:

> A ideia de garantir a revisão por pessoa natural de decisão automatizada gira em torno de corrigir eventuais discriminações decorrentes de processos algorítmicos e conferir mais transparência e *accountability* a processos de perfilamento dos cidadãos em perfis de consumo, profissionais ou de crédito. Em resumo, uma máquina não deveria ficar responsável por revisar uma decisão tomada por outra máquina. Desta maneira, o veto dado pela Presidência da República ao artigo da LGDP que visava garantir a revisão por pessoa natural, além de suprimir a possibilidade desse direito do cidadão, consequentemente também reduz a integralidade do acesso à justiça. (COALIZÃO DIREITOS NA REDE, 2019)

Desta forma, a eliminação da revisão humana a partir da instituição deste veto tornou a insegurança jurídica sobre o tema ainda mais significativa. O §1º do art. 20, por outro lado, facilita o exercício dos direitos do titular ao estabelecer que o controlador dos dados deverá fornecer, quando requerido, "informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial" (BRASIL, 2018). Essa facilitação, no entanto, é limitada pelo próprio dispositivo em questão, ao estabelecer que deverão ser salvaguardados o segredo comercial e o industrial.

Nessa perspectiva, Frank Pasquale (2015), em "*The black box society: The secret algorithms that control money and information*", alerta sobre os riscos da denominada "caixa preta de algoritmos" que traz opacidade ao processo de tratamento de dados. Ocorre que a Lei, ao ressalvar os segredos comercial e industrial, pode acabar endossando estratégias comerciais e de vigilância que apenas acentuam o desnivelamento entre o usuário e os operadores de dados. Enrico Roberto, no entanto, destaca que

> existem diversos mecanismos para averiguar se decisões automatizadas estão sendo justas e respeitando os princípios da lei sem a quebra do segredo de negócio. Dentre eles, informações como os tipos de dados que são usados para alimentar a base de dados, quais decisões de fato são tomadas por algoritmos, como elas podem afetar direitos fundamentais, quais populações afetadas pela decisão automatizada, bem como informar quais testes foram feitos com aquele algoritmo para evitar discriminações. (ROBERTO, 2020)

[28]A Coalizão Direitos na Rede é uma rede independente de organizações da sociedade civil, ativistas e acadêmicos em defesa da Internet livre e aberta no Brasil. Formada em julho de 2016, busca contribuir para a conscientização sobre o direito ao acesso à Internet, a privacidade e a liberdade de expressão de maneira ampla. O coletivo atua em diferentes frentes por meio de suas organizações, de modo horizontal e colaborativo.

O §2º do artigo 20 da LGPD também serve ao propósito de minorar possíveis danos causados pelo adendo trazido pelo §1º ao estabelecer que, em caso de não fornecimento das informações com base no sigilo, a Autoridade Nacional de Proteção de Dados (ANPD) poderá realizar auditoria para verificar a existência de aspectos discriminatórios (BRASIL, 2018). Por essa razão, a transparência torna-se um dos pontos centrais quando são analisadas as decisões automatizadas. Pode-se afirmar que, majoritariamente, o titular não tem conhecimento sobre como seus dados são coletados e de que modo serão destinados esses dados, tornando os riscos inerentes à sua utilização potencialmente maiores (BUFULIN, PIRES, 2020). Destaca-se que as decisões automatizadas deverão ser avaliadas ainda que não existam ameaças a direitos fundamentais para que se verifique como estas estão sendo utilizadas e se seu uso está sendo benéfico (BIONI, MARTINS, 2020)

Importa salientar, por fim, que o conjunto de princípios trazidos na LGPD são de relevância inegável. Tendo em vista que nenhuma legislação é capaz de prever todas as situações fáticas possíveis, os princípios apresentam-se como comandos orientadores para melhor aplicação do Direito. Neste sentido, os princípios elencados no art. 6º da LGPD servirão de apoio para que seja realizado controle sobre as decisões automatizadas, sobretudo, através dos princípios da finalidade, transparência, segurança, prevenção e não discriminação. Assim, mais uma vez destaca-se o papel central dos princípios na Lei Geral de Proteção de Dados: se por um lado houve prejuízo quando a reforma legislativa da Lei retirou o direito de revisão das decisões automatizadas por pessoa natural, por outro, os princípios criaram "uma espécie de pacote de direitos contra a tirania das decisões automatizadas" (BUFULIN, PIRES, 2020).

3. Considerações finais

Com o rápido avanço tecnológico, sistemas de inteligência artificial têm se tornado cada vez mais presentes em nosso cotidiano. Aplicáveis às mais diversas esferas da vida, algoritmos baseados em IA já exercem relevante papel no que diz respeito à tomada de decisões que afetam diretamente bilhões de pessoas. Não obstante, o desenvolvimento dessas novas tecnologias muitas vezes não leva em consideração importantes fatores, como desigualdades de gênero, de raça e culturais. Desta forma, tem-se como resultado o enviesamento de algoritmos que pode tornar o processamento de dados pessoais inadequado e discriminatório.

O enviesamento de algoritmos que regem decisões automatizadas eleva a

gravidade da situação que se afigura. Constata-se que as decisões automatizadas passam a integrar cada vez mais a sociedade, fazendo-se presente em âmbitos nucleares do indivíduo contemporâneo, permeando searas como a da educação, saúde, trabalho, crédito, sociabilidade e lazer. Destarte, violações de dados pessoais adquirem um potencial lesivo imensuravelmente maior, atingindo, inevitavelmente, a coletividade. Desponta, assim, a necessidade de proteção legal adequada.

Acompanhando a tendência mundial, a LGPD, inspirada no RGPD, representa um grande avanço na proteção da privacidade e intimidade dos titulares dos dados pessoais no Brasil. A adequação de processos tomadas de decisão baseadas em IA aos pressupostos éticos e jurídicos é, evidentemente, condição inegociável. A LGPD preconiza direitos indispensáveis, como o de revisão e explicação, bem como impõe a necessidade de transparência e interferência da ANPD. Ainda que passível de críticas, a Lei, no entanto, aumenta o arcabouço de garantias legais e passa a ser o principal mecanismo de governança em matéria de proteção de dados no país.

A escrita dos algoritmos computacionais, especialmente em decisões criminais, deve ser acompanhada pela sociedade e pelas instituições representativas das pessoas em situação de vulnerabilidade. O Conselho Nacional da Defensoria Pública, quando criado, poderá editar diretrizes de atuação para toda a classe dos Defensores Públicos, de modo a não permitir que a seletividade penal promova índices ainda maiores de encarceramento das minorias periféricas que os observados atualmente. Também poderá, após o novo desenho institucional, apoiar as políticas públicas com o uso positivo do *big data*, como no caso da distribuição de medicamentos para a população carente, com economia para os cofres públicos a partir do ganho de eficiência com a tecnologia (LARA; OLIVEIRA, 2017).

A "datificação" do comportamento humano em grande expressão é marca indelével de nosso tempo e se acentuará ainda mais num futuro breve, afetando em grande medida a forma dos seres humanos de relacionarem-se com o próximo e com os meios tecnológicos. Projetos baseados em big data já mostraram seu valor na área da saúde (previsão de disseminação de doenças), no planejamento urbano, no controle da criminalidade (alguns casos com sucesso, outros de uma vigilância assustadora) e até na prevenção do suicídio pelas redes sociais. Nem tudo são trevas no horizonte (LARA, 2019, p. 168).

4. Referências bibliográficas

AFP (AGENCE FRANCE-PRESSE). Tecnologia de reconhecimento facial apresenta erros, aponta estudo dos EUA. **Estado de Minas Internacional**, [*s.l.*], 19 dez. 2019. Disponível em: http://www.em.com.br/app/noticia/internacional/2019/12/19/interna_internacional,1109560/tecnologia-de-reconhecimento-facial-apresenta-erros-aponta-estudo-dos.shtml. Acesso em: 22 mar. 2021.

ANGWIN, Julia; KIRCHNER, Lauren; LARSON, Jeff; MATTU, Surya. Machine Bias: There's software used across the country to predict future criminals. **And it's biased against blacks**. ProPublica, 23 mar. 2016. Disponível em: http:// www.propublica.org/article/machine-bias-riskassessments-in-criminal-sentencing. Acesso em: 15 mar. 2021.

BARSS, Patchen. Can we eliminate bias in AI? How Canada's commitment to multiculturalism could help it become a world leader. **University of Toronto Magazine**. Toronto, 2019. Disponível em: http://www.utoronto.ca/news/can-we-eliminate-bias-ai-how-canada-s-commitment-multiculturalism-could-help-it-become-world. Acesso em: 02 mar. 2020.

BENJAMIN, Ruha. Retomando nosso fôlego: estudos de ciência e tecnologia, teoria racial crítica e a imaginação carcerária. In: SILVA, Tarcízio (org.). **Comunidades, algoritmos e ativismos digitais:** olhares afrodiaspóricos. São Paulo: Literatura, 2020.

CARRERA, Fernanda. Racismo e sexismo em bancos de imagens digitais: análise de resultados de busca e atribuição de relevância na dimensão financeira/profissional. In: SILVA, Tarcizio. **Comunidades, algoritmos e ativismos digitais**. São Paulo: LiteraRua, 2020.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

BIONI, Bruno Ricardo, MARTINS, Pedro. **Série LGPD em Movimento:** LGPD e decisões automatizadas. 2020. Disponível em: http://www.observatorioprivacidade.com.br/2020/12/14/serie-lgpd-em-movimento-lgpd-e-decisoes-automatizadas/#:~:text=O%20direito%20de%20revis%C3%A3o%20de%20decis%C3%B5es%20automatizadas%2C%20previsto%20pelo%20art.&text=Contudo%2C%20no%20processo%20de%20aprova%C3%A7%C3%A3o,feito%20por%20uma%20pessoa%20natural. Acesso em: 01 abr. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018a. **Lei geral de proteção de dados pessoais**. Brasília, Disponível em: http://bit.ly/30gadfD. Acesso em: 10 abr. 2021.

BUFULIN, Augusto Passamani, PIRES, Mariah Ferrari. **A sujeição às decisões automatizadas a partir da Lei Geral de Proteção de Dados**. 2020. Disponível

em: http://periodicos.uniformg.edu.br:21011/ojs/index.php/cursodireitouniformg/article/view/1224/1136. Acesso em: 02 abr. 2021.

FERNANDES, William Reis, SILVA, Rodrigo Cezario. **Aprendizagem profunda de máquinas: conceitos, técnicas e bibliotecas.** 2018. Disponível em: http://www.researchgate.net/profile/William-Fernandes/publication/324844857_Aprendizagem_profunda_de_maquinas_conceitos_tecnicas_e_bibliotecas/links/5ae77a8245851588dd7f86fa/Aprendizagem-profunda-de-maquinas-conceitos-tecnicas-e-bibliotecas.pdf. Acesso em: 01 abr. 2021.

FERRARI, Isabela, BECKER, Daniel. Direito à explicação e decisões automatizadas: reflexões sobre o princípio do contraditório. In: NUNES, Dierle, LUCON, Paulo Henrique dos Santos, WOLKART. Erik Navarro. **Inteligência Artificial e Direito Processual.** 2. ed. São Paulo: JusPodvm, 2021.

FRAZÃO, Ana. **Controvérsias sobre direito à explicação e à oposição diante de decisões automatizadas.** 2018a. Disponível em: http://bit.ly/2KIbWFn. Acesso em: 07 abri. 2021.

FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** 1. ed. São Paulo: Thomson Reuters Brasil, 2019.p.103.

FRAZÃO, Ana. **O direito à explicação e à oposição diante de decisões totalmente automatizada.** 2018b. Disponível em: http://bit.ly/2Hd86Sy. Acesso em: 07 abr. 2021.

GILLESPIE, Tarleton. The Relevance of Algorithms. *In* GiLLESPIE, Tarleton, Boczkowski, Pablo and Kirsten Foot, Media Technologies: **Essays on Communication, Mteriality, and Society**. Cambridge, MA: MIT, 2014.

GUEDES, Paula. Discriminação tecnológica: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes. **Grupo de Pesquisa de Direito do Instituto de Tecnologia e Sociedade 2020.** Disponível em: http://itsrio.org/wp-content/uploads/2020/10/Discrimina%C3%A7%C3%A3o-tecnol%C3%B3gica_Paula_Guedes.pdf. Acesso em: 03 mar 2021.

HILDEBRANDT, Mireille. **Privacy as protection of the incomputable self:** from agnostic to agonistic machine learning. Theoretical Inquiries of Law, v. 20, n. 1, 2019.

LARA, Caio Augusto Souza. **O acesso tecnológico à justiça**: por um uso contra hegemônico do *big data* e dos algoritmos. Belo Horizonte, 2019. Tese (doutorado) Universidade Federal

de Minas Gerais, Faculdade de Direito. Disponível em: http://repositorio.ufmg.br/handle/1843/DIRS-BC6UDB. Acesso em: 15 mar. 2021.

LARA, Caio Augusto Souza; OLIVEIRA, Alfredo Emanuel Farias de Oliveira. O *big data* e as políticas públicas de acesso à justiça: ideias para a constituição do Conselho Nacional da Defensoria Pública. In: **Acesso à Justiça II**. Coordenadores: Luiz Fernando Bellinetti; Regina Vera Villas Boas – Florianópolis: CONPEDI, 2017. Disponível em: http://www.conpedi.org.br/publicacoes/27ixgmd9/k8u53hoo/g1l81U3Z1WvvdD0u.pdf. Acesso em: 15 mar. 2021.

MCCURRY, Justin. South Korean woman's hair 'eaten' by robot vacuum cleaner as she slept. **The Guardian**, Tóquio, 9 fev. 2015. Disponível em: http://www.theguardian.com/world/2015/feb/09/south-korean-womans-hair-eaten-by-robot-vacuum-cleaner-as-she-slept. Acesso em: 15 mar. 2021.

MONARD, Maria Carolina, BARANAUSKAS, José Augusto. **Conceitos Sobre Aprendizado de Máquina. Sistemas Inteligentes Fundamentos e Aplicações**. 1 ed. Barueri-SP: Manole Ltda, 2003. p. 89.

MONTEIRO, Renato. 2018. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé**. Disponível em: http://bit.ly/2ZftSPz. Acesso em: 04 abr. 2021.

MULHOLLAND, C. **Dados pessoais sensíveis e a tutela de Direitos Fundamentais**. Uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18). R. Dir. Gar. Fund., Vitória, 2018, v. 19, n. 3.

NEGRI, S. M. C. A.; OLIVEIRA, S.R.; COSTA, R. S. O Uso de Tecnologias de Reconhecimento Facial Baseadas em Inteligência Artificial e o Direito à Proteção de Dados. **Revista Direito Público**, Brasília, v. 17, n. 93, p. 82-103, maio/jun., 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740. Acesso em: 22 mar. 2021.

PASQUALE, Frank. **The black box society. The secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

PASQUALE, Frank. **The black box Society.** Cambridge: Harvard University Press, 2015.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

ROBERTO, Enrico. **LGPD em Movimento: LGPD e decisões automatizadas**. Webinário realizado por Data Privacy Brasil. Disponível em http://www.youtube.com/watch?v=SNg8N7eCU6k&ab_channel=DataPrivacyBrasil. Acesso em: 02 abr. 2020.

ROSE, Adam. Are Face-Detection Cameras Racist?. **TIME**, [*s.l.*], 22 jan. 2010. Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html. Acesso em: 22 mar. 2021.

SALAS, Javier. Google conserta seu algoritmo "racista" apagando os gorilas. **El País**, [*s.l.*], 15 jan. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/01/14/tecnologia/1515955554_803955.html. Acesso em: 22 mar. 2021.

SILVA, Tarcízio**.** Racismo Algorítmico em Plataformas Digitais: microagressões e discriminação em código. In: SILVA, Tarcízio (org.). **Comunidades, algoritmos e ativismos digitais:** olhares afrodiaspóricos. São Paulo: Literatura, 2020.

VINCENT, James. AI is worse at identifying household items from lower-income countries. **The Verge**, [*s.l.*], 11 jun. 2019. Disponível em: http://www.theverge.com/2019/6/11/18661128/ai-object-recognition-algorithms-bias-worse-household-items-lower-income-countries. Acesso em: 22 mar. 2021.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho:** General Regulation Data Protection (Regulamento Geral sobre a Proteção de Dados). Bruxelas, 27 abr. 2016. Disponível em: http://bit.ly/2Ze3m4Y. Acesso em: 08 abr. 2021.

VOIGT, Paul; BUSSCHE, Axel von dem**. The EU General Data Protection Regulation (RGPD). A Practical Guide**. IT Governance Publishing; 3 ed. 2017.

A Proteção de Dados Pessoais à luz da Constituição Brasileira: Estudo de Caso sobre o Censo do IBGE (ADI N. 6387)

Gabriel Schulman[29]
Ana Carolina Contin Kosiak[30]

Brasil, meu nego
Deixa eu te contar
A história que a história não conta
O avesso do mesmo lugar
Na luta é que a gente se encontra[31]

RESUMO

O IBGE esclarece alguns princípios fundamentais sobre a adoção da Medida Provisória Nº 954. Essa Medida Provisória atende a pedido do Ministério da Economia, a partir de demanda técnica emergencial apresentada pelo IBGE. Para atender as recomendações de afastamento social do Ministério da Saúde e da OMS, o IBGE adiou o Censo Demográfico e suspendeu todas as suas pesquisas presenciais no dia 17 de março. Em função disso, para não comprometer a produção de indicadores e estatísticas sobre a economia, e fornecer um retrato fidedigno e atualizado sobre o País, o IBGE, como a maioria dos institutos de estatística do mundo, terá que migrar suas pesquisas para formas de coleta de dados não presenciais, adotando, principalmente, a coleta por telefone. Para isso o instituto necessita ter acesso aos dados (nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas) das operadoras telefônicas de modo a viabilizar a aplicação de suas pesquisas[32].

PALAVRAS-CHAVE

Proteção de Dados Pessoais; Audeterminação Informativa; Legalidade Constitucional; Constitucionalização do Direito.

[29] Doutor em Direito pela Universidade Estadual do Rio de Janeiro (UERJ). Mestre e Bacharel em Direito pela Universidade Federal do Paraná (UFPR). Especialista em Direito pela Universidade de Coimbra. Professor da Graduação e Mestrado Escola de Direito da Universidade Positivo (UP), onde também coordena o curso de Pós-Graduação em Direito e Tecnologia, e é líder do grupo "Pessoa, Tecnologia e Mercado". Advogado.

[30] Mestre e Bacharel em História pela Universidade Federal do Paraná (UFPR). Mestranda e Bacharel em Direito pela Universidade Positivo (UP).

[31] MANGUEIRA. **História pra ninar gente grande. Samba enredo de 2019**. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/carnaval/2019/noticia/2019/01/19/mangueira-veja-a-letra-do-samba-enredo-do-carnaval-2019-no-rj.ghtml>. Acesso em 05.11.2020.

[32] IBGE. **Comunicado sobre adoção da Medida Provisória 954/2020**. Disponível em: <https://www.ibge.gov.br/novo-portal-destaques/27477-comunicado-sobre-adocao-da-medida-provisoria-954-2020.html>. Acesso em 05.11.2020.

The protection of personal data in the light of the Brazilian Constitution: a case study on the IBGE census (ADI n. 6387)

ABSTRACT

The recognition of informative self-determination and protection of personal data as fundamental rights, by the Supremo Tribunal Federal (Brazilian Supreme Court), highlights its importance, unfolds in the need for reflection on the realization of these rights. Considering the legality of constitutional examination, the article investigates the judgment of ADI nº 6387, which considers the Medida Provisória (MP) nº 954 unconstitutional. The MP authorized access to telephone numbers and addresses of individuals or legal entities throughout Brazil, by IBGE (Brazilian Statistic and Geographic Institute), without specifying restrictions, precautions, and safeguards. The methodology refers to in the light of the Constitution as an interpretive process to implement these fundamental rights. Through the analysis, the interface between technology and protection of personal data were identified. As a synthesis of the results, the need of constitutional parameters for the resolution of conflicts in a constitutional interpretation of the LGPD, to avoid excesses, mitigate risks and offer adequate protection to the holders of personal data is defended.

KEYWORDS

Personal Data Protection; Informative Self-Determination; Constitutional Legality; Constitutionalization of Law.

Introdução

Em 17 de abril de 2020 foi editada a Medida Provisória nº 954/2020, que dispõe sobre o compartilhamento de dados por empresas de telecomunicações para o Instituto Brasileiro de Geografia e Estatística – IBGE. Por força da MP, as empresas de telefonia deveriam "disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" (art. 2º).

A medida provisória gerou absoluta controvérsia, e contou com dura oposição de diversas entidades. Tamanha a repercussão do tema, prontamente foram distribuídas cinco ações diretas de inconstitucionalidade (ADIs), promovidas por grupos de diferentes posições políticas[33] para discutir a (falta de) higidez constitucional da MP.

Neste contexto, elege-se como objeto de análise o acórdão proferido pelo Supremo Tribunal Federal por meio da ADI 6387[34], que reconheceu a inconstitucional material da Medida Provisória nº 954/2020. Dentre os vários temas que afloram do acórdão, o recorte proposto recai sobre a leitura à luz da Constituição, e o reconhecimento da proteção de dados como direito fundamental. Como percurso, inicia-se com um resgate da legalidade, ao que se segue a discussão do caso concreto julgado pelo STF e, por fim, extraem-se aprendizados úteis.

Sob o prisma metodológico, a escolha do caso do Censo do IBGE se justifica por variados fundamentos. Além da repercussão social e jurídica, consiste no primeiro caso em que o STF reconheceu expressamente a *autodeterminação informativa* como direito fundamental, bem como a primeira oportunidade em que tratou da Lei Geral de Proteção de Dados Pessoais (LGPD).

Salienta-se igualmente que na solução do caso, a despeito da menção expressa aos princípios da LGPD, o Supremo utilizou-se da leitura constitucional. Como se exporá ao longo na seção seguinte, a legalidade constitucional rejeita qualquer possibilidade de interpretação que não seja à luz da Constituição. De todo modo, o exame do acórdão auxilia na compreensão da sistemática interpretativa e afasta alguns argumentos frágeis

[33] As ações diretas de inconstitucionalidade que, questionam o repasse das informações de empresas telefônicas ao IBGE, estabelecido pela MP 954/2020 foram propostas pela Ordem dos Advogados do Brasil (ADI 6387) e pelos partidos políticos PSDB (ADI 6388), PSB (ADI 6389), PSOL (ADI 6390), e PCdoB (ADI 6393). Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=441728 Considerando que as ações diretas de inconstitucionalidade igualmente impugnam a validade constitucional da Medida Provisória n. 954/2020, determinou-se a tramitação conjunta dos feitos, e com a reprodução da decisão da ADI 6387 nos demais casos.

[34] STF. **ADI n. 6387**. Relª. Minª. Rosa Weber. Tribunal pleno. Dje: 11.11.2020.

como a visão de que o texto constitucional não possuísse força normativa, fosse excessivamente abstrato ou tivesse aplicação subsidiária[35].

É inevitável também a comparação do caso do censo brasileiro com o julgamento pela Corte Alemã, que considerou inconstitucional a Lei do Censo de 1982[36]. A despeito das diferenças de contexto, de sistemas jurídicos, os casos apresentam interessantes pontos de contato, eis que, além de versarem sobre o uso de dados sobre censo, permitiram aos julgadores se debruçarem, à luz da constituição, sobre a finalidade do emprego de dados pessoais, autodeterminação e o caráter imperioso de sua proteção.

É interessante perceber que, na Alemanha, também se julgou um caso de proteção de dados pessoais envolvendo o censo e os dados que lá se pretendia coletar. Trata-se de conhecido precedente sobre o qual se apresentam considerações mais adiante. No tocante ao caso brasileiro, sob uma perspectiva de leitura à luz da Constituição, três aspectos merecem serão aprofundados no exame do julgamento do caso pelo STF.

Em primeiro, entre os fundamentos relevantes da decisão está a regra da proporcionalidade, a qual, embora consagrada na jurisprudência nacional, é reforçada na LGPD, como denota, inclusive, a previsão dos princípios da necessidade, adequação e proporcionalidade, além de diversas outras normas que os reforçam. Nessa linha, defende-se que a LGPD, além de guiar-se pelo direito fundamental ao tratamento de dados pessoais, ao estabelecer tais princípios, institui um importante acervo de filtros relevantes na depuração do tratamento dos dados pessoais.

Em segundo, a decisão do STF sublinhou o reconhecimento da proteção de dados como direito fundamental, o que repercute nas relações cidadão-Estado e nas relações entre particulares. Em terceiro, a solução do caso se restringe a acolher, como base normativa, "apenas" a LGPD ou o texto constitucional. Essa compreensão ampla e integrada das normas jurídicas, que leva em conta os diversos diplomas legais se coaduna com o reconhecimento de um marco normativo mais amplo de proteção de dados pessoais no direito brasileiro, consentâneo à noção de ordenamento unitário e complexo, que não isola textos legislativos para casos ou situações específicas, orienta-se por um conjunto mais denso de normas, em sintonia com o texto constitucional.

[35] FLÓREZ-VALDÉS, Joaquín Arce y. **El derecho civil constitucional**. Madrid (Espanha): Civitas, 1991. p. 89-94.
[36] MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. ***Revista Direitos Fundamentais & Justiça*****,** a. 12, n. 39, p. 185-216, jul./dez. 2018.

Diante de tal cenário, procura-se, na próxima seção, revisitar a leitura à luz da constituição como processo interpretativo necessário à proteção de dados pessoais, bem como, ao longo do artigo, apreender a maneira como foi aplicada no julgamento deste importante precedente pelo Supremo Tribunal Federal.

1. Legalidade constitucional: "premissas metodológicas a caminho do direito civil constitucional"

A *legalidade constitucional* em sua essência implica um duplo movimento. Em primeiro, tem por pressuposto o reconhecimento da força normativa da Constituição, inclusive dos direitos fundamentais[37]; em segundo, assinala que as normas constitucionais "condicionam a validade e o sentido de todo ordenamento jurídico"[38]. Tal perspectiva traduz, portanto, a necessidade de uma leitura axiológica, finalística, que toma as normas constitucionais como bússola. Dessa maneira, em face da legalidade constitucional "tudo encontra validade e legitimidade no sistema constitucional"[39].

Do ponto de vista do conteúdo, consagra os direitos fundamentais e a promoção da pessoa concreta. Como norte da legalidade constitucional, estão a centralidade da pessoa, a promoção da dignidade da pessoa humana[40], o desenvolvimento da sua personalidade, os direitos humanos e fundamentais[41]. Essa leitura do Direito constitui, ao mesmo tempo, uma *visão* e uma *metodologia interpretativa*, que se opõe à neutralidade dos intuitos[42], da hermenêutica estritamente literal[43], a despreocupada com a

[37] CANARIS, Claus-Wilhelm. A influência dos direitos fundamentais sobre o direito privado na Alemanha. In: SARLET, Ingo Wolfgang (Org.). **Constituição, Direitos Fundamentais e Direito Privado**. 2. ed. Porto Alegre: Livraria do Advogado, 2006. p. 225-245.

[38] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. Os conceitos fundamentais e a construção do novo modelo. 9. ed. Saraiva, 2019. Item 4.1. Em sentido similar: CANARIS, Claus-Wilhelm. **Direitos Fundamentais e Direito Privado**. Coimbra (Portugal): Almedina, 2006. p. 27-28.

[39] PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional.** Rio de Janeiro: Renovar, 2008. Prefácio a 1ª Edição. p. XXIII.

[40] BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**. **A construção de um conceito jurídico à luz da jurisprudência mundial**. Belo Horizonte: Fórum, 2014. NOVAIS, Jorge Reis. **A dignidade da pessoa humana. Dignidade e direitos fundamentais**. v. I, Coimbra: Almedina, 2015. MORAES, Maria Celina Bodin de. O conceito de dignidade humana. In*:* _____. **Princípios do direito civil contemporâneo**. Rio de Janeiro: Renovar, 2006. p. 1-60. NEVES, Maria do Céu Patrão. Sentidos da vulnerabilidade: característica, condição, princípio. **Revista Brasileira de Bioética**, *v*. 2. n. 02, p. 153-172, 2006.

[41] TEPEDINO Gustavo. Premissas metodológicas para a constitucionalização do direito civil. **Revista de Direito do Estado**, Bahia, ano 1, nº 2, abr./jun. 2006, p. 37-53.

[42] RAMOS, Carmem Lucia Silveira. Constitucionalização do direito privado e a sociedade sem fronteiras. In: FACHIN, Luiz Edson (Coord.). **Repensando fundamentos de Direito Civil Brasileiro Contemporâneo.** Rio de Janeiro: Renovar, 1998. p. 3-29. p. 6

[43] RODOTÀ, Stefano. **La vita e le regole**. Tra diritto e non diritto. 4. ed. Milão: Feltrini, 2007. p. 28.

fundamentação das normas e com seus impactos na realidade[44]. Busca-se a concretização de *normas-valores* como a dignidade da pessoa humana e a igualdade substancial[45].

Sob um ângulo técnico ou metodológico, faz-se necessário um conjunto de cuidados importantes que permitem atender a segurança jurídica material. Nessa toada, a utilização das aspas no título desta seção busca homenagear dois textos clássicos sobre o tema[46], os quais refletem um conteúdo atual e necessário ao apresentarem os fundamentos da interpretação-aplicação[47] do direito à luz da Constituição. Permita-se reiterar que é exatamente sob essa perspectiva que o STF estabeleceu as bases de sua análise do caso do censo do IBGE. Nessa linha, o acórdão, ao julgar a inconstitucionalidade da medida provisória sublinha que "a MP nº 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros".

Como se pode observar, a legalidade constitucional não se confunde com um recurso a uma noção vaga de constituição. No processo de interpretação-aplicação, o texto constitucional não é um mero adorno a enfeitar a aplicação das leis; é fonte normativa primária, direta, cuja força confere unidade ao ordenamento. O caráter irradiante das normas constitucionais significa que iluminam todo o ordenamento. Nessa linha, como expressou o Supremo, "todas as possíveis limitações a direitos e garantias individuais precisam seguir os parâmetros constitucionais de excepcionalidade, razoabilidade e proporcionalidade". Nessa seção, segue-se com a revisita à legalidade constitucional e suas premissas para facilitar o exame dos critérios adotados pela Corte para concluir pela inconstitucionalidade da MP.

---

[44] LÔBO, Paulo Luiz Netto. Constitucionalização do direito civil. **Revista de Informação Legislativa.** Brasília, Senado Federal, n. 141, ano 36, p. 99-109, jan./mar. 1999. p. 100.

[45] TEPEDINO, Gustavo. Crise das Fontes Normativas e Técnica Legislativa na Parte Geral do Código Civil de 2002. In: **A Parte Geral do Novo Código Civil**. 3. ed. Rio de Janeiro: Renovar, 2007. p. XV-XXXIII. "Se o direito e, sobretudo a Constituição, têm a sua eficácia condicionada aos fatos concretos da vida, não se afigura possível que a interpretação faça deles tábua rasa. Ela há de contemplar essas condicionantes, correlacionando-as com as proposições normativas da Constituição. A interpretação adequada é aquela que consegue concretizar de forma excelente, o sentido (Sinn) da proposição normativa dentro das condições reais dominantes numa determinada situação". HESSE, Konrad. **Força Normativa da Constituição.** Porto Alegre: Sergio Fabris, 1991. p. 22-23. Cf. também HERRERA FLORES, Joaquín. ¿Crisis de la ideología o ideología de la crisis? Respuestas neoconservadoras. Crítica Jurídica, **Revista Latino Americana de Política, Filosofía y Derecho**, UNAM/Instituto de Investigaciones Jurídicas, n. 13, p. 123-143, 1993.

[46] BODIN DE MORAES, Maria Celina. A Caminho de um Direito Civil Constitucional. **Revista de Direito Civil Imobiliário, Agrário e Empresarial**, São Paulo, vol. 65, ano 17, jul./set. 1993, p. 21-32. TEPEDINO Gustavo. Premissas metodológicas para a constitucionalização do direito civil. **Revista de Direito do Estado**, Bahia, ano 1, nº 2, abr./jun. 2006, p. 37-53.

[47] PERLINGIERI, Pietro. **Perfis do Direito Civil. Introdução ao Direito Civil Constitucional**. 2. ed. São Paulo: Renovar, 2002. p. 71.

A partir da compreensão da constitucionalização do direito, torna-se imprescindível e urgente a checagem da compatibilização da legislação com texto constitucional, em qualquer caso; afinal, não há interpretação em que a constituição não esteja presente, ainda que a solução seja obtida pela aplicação do texto normativo infraconstitucional. Por meio do controle de constitucionalidade, em todo e qualquer caso se promove a "filtragem constitucional"[48].

Na lição de Tepedino, a atividade interpretativa deve superar alguns graves preconceitos que o afastam de uma perspectiva civil-constitucional. Em primeiro lugar, trata sobre a necessária dissociação do texto constitucional como "carta política", porque isso, além de destituir a Constituição de seu papel unificador do direito privado, ainda o tornaria refém do legislador ordinário[49]. Depois, afirma que não se pode concordar com os "civilistas que se utilizam dos princípios constitucionais como princípios gerais de direito", uma vez que isso representaria uma "subversão da hierarquia normativa"[50].

Em terceiro lugar, o autor apresenta que, no que tange à técnica interpretativa, não se pode vincular à "necessidade de regulamentação casuística", justamente porque as constituições contemporâneas utilizam-se de cláusulas gerais que equivalem a "cláusulas jurídicas aplicáveis direta e imediatamente nos casos concretos"[51]. Por fim, defende que a "interpenetração do direito público e do direito privado" caracteriza a sociedade contemporânea, sendo que a perspectiva de interpretação civil-constitucional permite que sejam "revigorados os institutos de direito civil"[52]. Nesse passo, o julgamento do Supremo Tribunal Federal acerca do Censo sublinhou o reconhecimento da proteção de dados como direito fundamental, e da própria compreensão de que não há leitura do ordenamento que dispense a compreensão à luz da Constituição.

Ao tomar o ordenamento jurídico como "unitário complexo",[53] supera-se a clássica dicotomia entre direito público e direito privado, haja vista que não há zonas imunes aos direitos fundamentais. A leitura à luz da Constituição afasta a possibilidade destas áreas de sombra, e implica que as normas constitucionais penetram todas as áreas,

[48] SCHIER, Paulo Ricardo. **Filtragem Constitucional.** Construindo uma nova dogmática jurídica. Porto Alegre: Sergio Antonio Fabris, 1999.
[49] TEPEDINO, *Op. Cit*. p. 50.
[50] *Idem*.
[51] *Ibidem*, p. 51.
[52] *ibidem,* p. 51-52.
[53] PERLINGIERI, Pietro. **Perfis do Direito Civil. Introdução ao Direito Civil Constitucional.** 2. ed. São Paulo: Renovar, 2002. p. 6. Por essa razão, "o direito especial tem sua peculiaridade e sua limitada autonomia, mas sempre derivada e vinculada pelas diretrizes e valores do sistema". Obra citada, p. 79.

de maneira a consagrar os direitos fundamentais e priorizar os valores existenciais. Nas palavras de Bodin de Moraes:

> Acolher a construção da unidade (hierarquicamente sistematizada) do ordenamento jurídico significa sustentar que seus princípios superiores, isto é, os valores propugnados pela Constituição, estão presentes em todos os recantos do tecido normativo, resultando, em consequência, inaceitável a rígida contraposição direito público-direito privado. Os princípios e valores constitucionais devem se estender a todas as normas do ordenamento, sob pena de se admitir a concepção de um "*mondo in frammenti*", logicamente incompatível com a ideia de sistema unitário[54].

Para a autora, a regulamentação da atividade privada (porque regulamentação da vida cotidiana) deve ser, em todos os momentos "expressão da indubitável opção constitucional de privilegiar a dignidade da pessoa humana"[55]. Em consequência, delineia-se um "direito civil constitucionalizado", que se traduz em um direito civil "efetivamente transformado pela normativa constitucional"[56].

Em sintonia com tal perspectiva, ao julgar o Caso do Censo do IBGE, o STF sublinhou que esta compreensão foi essencial para a apreciação do Caso do Censo alemão, "por ter permitido que o direito à privacidade não mais ficasse estaticamente restrito à frágil dicotomia entre as esferas pública e privada, mas, sim, se desenvolvesse como uma proteção dinâmica e permanentemente aberta às referências sociais e aos múltiplos contextos de uso"[57].

Ao tomar o ordenamento jurídico como unitário complexo, supera-se a clássica dicotomia entre direito público e direito privado, haja vista que não há zonas imunes aos direitos fundamentais[58]. A leitura à luz da Constituição afasta a possibilidade destas áreas de sombra, e implica que as normas constitucionais penetram todas as áreas, de maneira a consagrar os direitos fundamentais e priorizar os valores existenciais.

Não se trata apenas de recorrer à Constituição para interpretar as normas ordinárias de direito civil (aplicação indireta), mas também de reconhecer que as normas constitucionais podem, e devem, ser diretamente aplicadas às relações jurídicas estabelecidas entre particulares. A rigor, para o direito civil-constitucional, não importa

---

[54] BODIN DE MORAES, Maria Celina. A Caminho de um Direito Civil Constitucional. **Revista de Direito Civil Imobiliário, Agrário e Empresarial**, São Paulo, vol. 65, ano 17, jul./set. 1993, p. 21-32. p. 24.
[55] *Ibidem*, p. 28.
[56] *Ibidem,* p. 29.
[57] STF. **ADI n. 6387**. Relª. Minª. Rosa Weber. Tribunal pleno. Dje: 11.11.2020.
[58] ZAGREBELSKY. **El Derecho Dúctil. Ley, Derecho, Justicia**. 8. ed. Madrid (Espanha): Editorial Trotta, 2008. p. 39-40. PERLINGIERI, Pietro. **Perfis do Direito Civil. Introdução ao Direito Civil Constitucional.** 2. ed. São Paulo: Renovar, 2002. p. 6. Por essa razão, "o direito especial tem sua peculiaridade e sua limitada autonomia, mas sempre derivada e vinculada pelas diretrizes e valores do sistema". Obra citada, p. 79.

tanto se a Constituição é aplicada de modo direto ou indireto (distinção nem sempre fácil)[59]. O que importa é obter a máxima realização dos valores constitucionais no campo das relações privadas.

Como ensina Maria Celina Bodin de Moraes, a metodologia civil-constitucional propõe uma "reconstrução do Direito a partir de princípios – que representam valores estabelecidos na Constituição"[60]. Em harmonia, Barroso afirma que os princípios expressam os valores fundamentais do sistema, dando-lhe unidade e condicionando a atividade do intérprete. Em um ordenamento jurídico pluralista e dialético, princípios podem entrar em rota de colisão. Em tais situações, o intérprete, à luz dos elementos do caso concreto, da proporcionalidade e da preservação do núcleo fundamental de cada princípio e dos direitos fundamentais, procede a uma ponderação de interesses[61].

A respeito, extrai-se do voto do Min. Alexandre de Moraes no acórdão que trata do julgamento do caso do Censo, "Em cada uma das hipóteses legais, ou mesmo judiciais, há que se analisar se, na hipótese, constam as necessárias adequações, razoabilidade e proporcionalidade" que seriam necessários para "excepcionalmente, relativizar-se a proteção constitucional ao sigilo de dados". Da mesma maneira, Perlingieri destaca a importância central da ponderação, técnica idônea a promover o sopesamento de todas as normas (e, sobretudo, dos princípios), para a solução de cada caso concreto[62]. À luz do conceito-chave da proporcionalidade, desenvolveu-se o método de ponderação pelo qual o magistrado, considerando-se a importância que os bens jurídicos cotejados têm, em tese, mas também as peculiaridades do caso concreto, poderá prover ao direito postulado, "fundamentando-se na precedência condicionada deste sobre os princípios contrapostos"[63].

Desse modo, integra-se ao acervo de ferramentas oferecidas pela leitura constitucional a incidência da regra da proporcionalidade. Sem adentrar na interessante controvérsia da literatura jurídica sob as etapas aplicáveis à proporcionalidade, ou sua diferenciação em relação à razoabilidade[64], acolhe-se o ensinamento de Luís Roberto

[59] SCHREIBER, Anderson; KONDER, Carlos Nelson. Uma agenda para o direito civil-constitucional. **Revista Brasileira de Direito Civil**, vol. 10, out./dez. 2016.
[60] BODIN DE MORAES, Maria Celina. Do juiz boca-da-lei à lei segundo a boca-do juiz: notas sobre a aplicação-interpretação do direito no início do Século XXI. **Revista de Direito Privado**, São Paulo, ano 14, vol. 56, p.11-30, out./dez. 2013. p. 19.
[61] BARROSO, Luís Roberto. Fundamentos Teóricos e Filosóficos do Novo Direito Constitucional Brasileiro. **Revista da EMERJ**, vol. 4, n. 15, 2001, p. 1-47. p. 27.
[62] PERLINGIERI, Giovanni. **Profili applicativi della ragionevolezza nel diritto civile**. Napoli: Edizioni Scientifiche Italiane, 2015. p. 68.
[63] BARROSO, *Op. Cit.*, p. 27.
[64] SILVA, Virgílio Afonso. O proporcional e o razoável. **Revista dos Tribunais**, v. 798, p. 23-50, 2002. p.

Barroso que esclarece que o "princípio da razoabilidade ou proporcionalidade" traduz-se em um teste que permite o exame dos atos e invalidá-los quando:

> a) não haja adequação entre o fim perseguido e o instrumento empregado (*adequação*);
> b) a medida não seja exigível ou necessária, havendo meio alternativo menos gravoso para chegar ao mesmo resultado (*necessidade/vedação do excesso*);
> c) não haja proporcionalidade em sentido estrito, ou seja, o que se perde com a medida é de maior relevo do que aquilo que se ganha (*proporcionalidade em sentido estrito*)[65].

Dessa maneira, no exercício de restrições ao direito fundamental à proteção de dados, com base no critério da *necessidade*, deve-se considerar se o objetivo pode ser atingido com menor limitação de direitos fundamentais[66].

A *constitucionalização* marca, pois, não uma alteração perfunctória, mas de fundo[67]. Não se trata apenas de uma troca de fontes[68], mas da construção de um sistema plural, complexo, pautado na concretude, eis que centrado na pessoa e na adequada atenção às vulnerabilidades[69]. Sob o prisma interpretativo "a interpretação axiológica representa a superação histórica e cultural da interpretação literal"[70]. Sob o prisma metodológico – ao qual, é certo, o anterior não está despegado – a interpretação sofre uma

---

40.

[65] BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. Os conceitos fundamentais e a construção do novo modelo. 9. ed. São Paulo: Saraiva, 2019. Item 4.5. Com compreensão similar: SARMENTO, Daniel. Os Princípios Constitucionais e a Ponderação de Bens. *In:* TORRES, Ricardo Lobo. (Org.). **Teoria dos Direitos Fundamentais**. Rio de Janeiro: Renovar, 1999. p. 35-93. p. 58. Para outras compreensões sobre o tema, confrontar: SILVA, Virgílio Afonso. O proporcional e o razoável, **Revista dos Tribunais**, v. 798, p. 23-50, 2002. Humberto Ávila também diferencia razoabilidade e o "postulado da proporcionalidade", que não designa de princípio. ÁVILA. Humberto. **Teoria dos Princípios**. Da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Malheiros, 2005, p. 108-115. ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2008.

[66] SILVA, Virgílio Afonso. O proporcional e o razoável. **Revista dos Tribunais**, v. 798, p. 23-50, 2002. p. 40.

[67] Aduz PERLINGIERI: "A harmonização entre fontes exige por parte do jurista um esforço constante, contínuo, em grande parte ainda a ser concretizado. A hierarquia das fontes não responde apenas uma expressão de certeza formal do ordenamento para resolver os conflitos entre as normas emanadas de diversas fontes; é inspirada, sobretudo, em uma lógica substancial, isto é, nos valores e na conformidade da filosofia da vida presente no modelo constitucional". PERLINGIERI, Pietro. **Perfis do Direito Civil.** Introdução ao Direito Civil Constitucional. 2. ed. Rio de Janeiro: Renovar, 2002. p. 9-10.

[68] Segundo Pietro SANCHÍS: "*La Constitución no ha venido simplemente a ocupar el papel de la ley, sino a diseñar un modelo de producción normativa notablemente más complejo, donde todos los sujetos encuentran, no un orden jerárquico unívoco, sino orientaciones de sentido conflictivo que exigen ponderación*". SANCHÍS, Luis Pietro. **Constitucionalismo y Positivismo.** 2. ed. México: Fontamara, 1999. (Biblioteca de Ética Filosofía del Derecho y Política, v. 60). p. 36.

[69] BARBOZA, Heloisa Helena. Vulnerabilidade e cuidado: aspectos jurídicos. In: PEREIRA, Tânia; OLIVEIRA, Guilherme de (coord.). **Cuidado e vulnerabilidade.** São Paulo: Atlas, 2009, p. 106-118. BARBOZA, Heloísa Helena. Reflexões sobre autonomia negocial. In: TEPEDINO, Gustavo, FACHIN, Luiz Edson (coord.). **O direito e o tempo**: embates jurídicos e utopias contemporâneas – Estudos em homenagem ao Professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008.

[70] PERLINGIERI, Pietro. **Perfis do Direito Civil.** Introdução ao Direito Civil Constitucional. 2. ed. Rio de Janeiro: Renovar, 2002. p. 73.

virada[71] significativa, alterando seu ponto de referência[72], de modo que "a mudança de atitude é substancial: deve o jurista interpretar o Código Civil segundo a Constituição e não a Constituição de acordo com Código, como ocorria com freqüência (e ainda ocorre)"[73].

Deve prevalecer, dessa maneira, a compreensão segundo a qual o Direito contemporâneo encontra sua unidade ou integridade na axiologia constitucional[74]. Portanto, o que explica o Direito contemporâneo é ser, conforme reflete Perlingieri, unitário e complexo:

> *è indispensabile concepire l'ordinamento giuridico come unitario e complesso, là dove i princípi costituzionali fungono da valori guida e assumono un ruolo di baricentro nell'articolata pluralità delle fonti del diritto. Ciò esclude che si possa configurare il sistema ordinamentale diviso in branche autonome o in tanti microsistemi policentrici, in ranghi o livelli normativi tra loro separati e non comunicabili*.[75]

---

[71] A referência à *Virada* se fez em homagenm à obra: FACHIN, Luiz Edson (Coord.). **Repensando fundamentos de Direito Civil Brasileiro Contemporâneo.** Rio de Janeiro: Renovar, 1998. e ao Núcleo de Pesquisa de Direito Civil da UFPR – Projeto "Virada de Copérnico". Sobre a "virada" confira-se, entre outros artigos: FACHIN, Luiz Edson. "Virada de Copérnico"; um convite à reflexão sobre o Direito Civil brasileiro contemporâneo. In: _____. (Coord.). **Repensando fundamentos de Direito Civil Brasileiro Contemporâneo.** Rio de Janeiro: Renovar, 1998. p. 317-324.

[72] Consoante TEPEDINO: "[...] é de se buscar a unidade do sistema, deslocando para a tábua axiológica da Constituição da República o ponto de referência antes localizado no Código Civil". TEPEDINO, Gustavo. Premissas Metodológicas da Constitucionalização do Direito Civil. In: _____. **Temas de Direito Civil**. v. I. 2. ed. rev. atual. Rio de Janeiro: Renovar, 2001. p. 1-22. p. 13.

[73] LÔBO, Paulo Luiz Netto. Constitucionalização do direito civil. **Revista de Informação Legislativa.** Brasília, Senado Federal, n. 141, ano 36, p. 99-109, jan./mar. 1999. p. 100.

[74] Destarte, "o papel unificador do sistema, tanto em seus aspectos mais tradicionalmente civilísticos quanto naqueles de relevância publicista, é desempenhado de maneira cada vez mais incisiva pelo Texto Constitucional". PERLINGIERI, Pietro. **Perfis do Direito Civil.** Introdução ao Direito Civil Constitucional. 2. ed. Rio de Janeiro: Renovar, 2002. p. 6. Nesse sentido, também as idéias lançadas por Gustavo TEPEDINO, Luiz Edson FACHIN, Paulo LÔBO, Maria Celina Bodin de MORAES. Desta última, em especial: TEPEDINO, Maria Celina Bodin de Moraes. A caminho de um Direito Civil Constitucional. **Revista de Direito Civil Imobiliário, Agrário e Empresarial,** São Paulo: RT, v. 65, ano 17, p. 21-32, jul./set. 1993.

[75] PERLINGIERI, Pietro. **La dottrina del diritto civile nella legalità costituzionale**. Conferência Magna proferida por ocasião do Congresso de Direito Civil Constitucional da Cidade do Rio de Janeiro. Rio de Janeiro: 21/09/2006. Em tradução livre: "é indispensável que se conceba o ordenamento jurídico como unitário e complexo, em que os princípios constitucionais funcionam como valores guias e assumem um rol de baricentro na articulada pluralidade de fontes do direito. Isto é, exclui-se que se possa configurar um sistema ordinariamente dividido em ramos autônomos ou em tantos microssistemas policêntricos, em classes ou níveis normativos entre si separados e incomunicáveis". Ao examinar o monismo estatal na produção da lei a culminar na limitação da juridicidade ao plano da validade, acentua GROSSI: "Hoje, adverte-se sobre a decrepitude deste castelo de outros tempos, absolutamente inadequado com o seu fosso isolador, a sua ponte levadiça, as muralhas interrompidas por mínimas aberturas no alto. Deixando de lado as imagens evocadoras, não se pode mais eximir da verificação de que o mundo inteiro corre em uma direção que já não é mais aquela do encerramento na couraça da validade, mas de uma valorização do oposto princípio da efetividade; veja-se a carga vital de certos fatos e sua incisividade no social, está determinada pelas suas próprias forças interiores. Efetividade mais do que validade, tem-se como resultado imediato o abandono do velho e inadequado monismo jurídico para uma abertura substancialmente pluralista, já que é unitário e compacto o reino do válido, heterogêneo, plural, complexo é, ao contrário, o reino do efetivo". GROSSI, Paolo. A formação do jurista e a exigência de um hodierno "repensamento" epistemológico. (Trad. Ricardo Marcelo Fonseca). **Revista da Faculdade de Direito da UFPR,** Curitiba,

A partir do exposto, a perspectiva adotada no presente artigo adota os seguintes pressupostos, oferecidos aqui como uma espécie de síntese da ordem de ideias exposta:

> **i.** A Constituição, toda ela, é norma, juridicamente eficaz. O reconhecimento da força normativa do texto constitucional engloba suas regras, princípios e os direitos fundamentais;
> **ii.** Diante da supremacia do texto constitucional sua aplicação não depende de norma ordinária;
> **iii.** Na interpretação do direito é indispensável a filtragem constitucional; toda interpretação deve ser constitucional;
> **iv.** O texto normativo não é um dado, é um construído e deve atender, entre outros critérios, a promoção da pessoa e a proteção do vulnerável;
> **v.** Nenhuma leitura do texto originário é uma leitura que não seja do texto constitucional;
> **vi.** O ordenamento é complexo e unitário; a legislação setorial é relevante, mas não se pode isolar normas como se fossem ilhas incomunicáveis no sistema jurídico;
> **vii.** O direito deve buscar a concretização dos direitos fundamentais, levar em conta os impactos concretos das interpretações e distanciar-se das abstrações;
> **viii.** O direito deve buscar, também, uma leitura funcionalizada, que sem desprezar as categorias formais e a estrutura dos institutos jurídicos os insere em uma realidade concreta de modo que *Law in Books* não se feche a realidade;
> **ix.** À luz da historicidade, reconhece-se que os significados dos significantes se transformam ao longo do tempo[76]; o exame dos institutos do passado (e do presente) demanda sua compreensão em harmonia com a Constituição e com o mundo que não apenas os circunda, mas no qual se inserem. Não se pode estancar o Direito, descambando em soluções estáticas.

Dessa maneira, a leitura constitucional pressupõe um enfoque na melhor proteção da pessoa, efetivando e promovendo os direitos fundamentais, os direitos humanos e a proteção da pessoa humana – além dos valores constitucionais e os objetivos da República. Ainda, a premissa da interpretação à luz do texto constitucional expõe que não existem estatutos isolados no ordenamento jurídico, mas que, por outro lado, todas as normas devem ser aplicadas e analisadas em conjunto. Nesse sentido, deve-se analisar a Lei Geral de Proteção de Dados, por exemplo, e a todo momento, à luz da Constituição.

Algumas leis, inclusive, fazem referência à aplicação constitucional em seu próprio texto normativo como verifica-se na própria LGPD ao reproduzir expressamente diversos princípios constitucionais. Tal repetição é desnecessária, a Constituição não é

UFPR, v. 40, p .6-25, 2004. p. 15.
[76] FACHIN, Luiz Edson. **Direito Civil. Sentidos, transformações e fim.** Rio de Janeiro: Renovar, 2015. p. 60-65.

afastada pela lei ordinária, a quem só resta obedecer. Em contrapartida, a repetição de princípios e regras constitucionais na LGPD termina por reforçar a leitura aqui proposta.

2. O caso concreto: discussão objeto da Ação Direta de Inconstitucionalidade nº 6.387

Conforme exposto, a Medida Provisória nº 954/2020 determinava um vasto compartilhamento de dados com o IBGE com o intuito de dar suporte à produção estatística oficial durante a pandemia de COVID-19. Sem prejuízo à reconhecida importância do instituto e da realização do censo, foram opostas diversas ações diretas de inconstitucionalidade para discutir sua (in)constitucionalidade.

Em termos práticos, a medida provisória implicava que as empresas de telecomunicação seriam obrigadas a enviar ao IBGE **a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas, para "produção estatística oficial" e "entrevistas em caráter não presencial no âmbito de pesquisas domiciliares". Apontou o Conselho Federal da OAB, em síntese, que a MP:**

> a) viola dados sigilosos, inclusive o telefônico, de todos os brasileiros; b) tem como finalidade informada, de modo genérico e impreciso, a produção de estatística oficial mediante a realização de entrevistas não presenciais no âmbito de pesquisas domiciliares; c) estabelece a guarda dos dados disponibilizados no âmbito da Fundação IBGE, sem definir procedimentos de controle pelo Judiciário, pelo Ministério Público ou por órgãos da sociedade civil; d) não apresenta com precisão a modalidade, a frequência e o objetivo das pesquisas a serem realizadas; e) não aponta razões justificadoras da urgência e da relevância da medida; f) não apresenta razões que justifiquem a necessidade do compartilhamento dos dados para a pesquisa estatística; g) silencia sobre a adoção de mecanismo de segurança para reduzir o risco de acesso e uso indevidos; e h) ao prever a elaboração de relatório de impacto após o uso dos dados, e não previamente ao compartilhamento, impede a efetiva avaliação dos riscos[77].

A petição inicial, no que se refere à inconstitucionalidade material da MP, considerou como indiscutível, na ordem constitucional brasileira, o direito fundamental à proteção de dados pessoais, essencial para assegurar a tutela da intimidade e da vida privada[78]. Em consonância, afirmou que, do mesmo dispositivo constitucional, é possível extrair a existência de um direito fundamental à autodeterminação informativa – direito

[77] STF. Ação Direta de Inconstitucionalidade (ADI) com pedido cautelar proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), perante o Supremo Tribunal Federal (STF), em face da integralidade dos dispositivos estabelecidos pela Medida Provisória nº 954, de 17 de abril de 2020. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=752502168&prcID=5895165#>. Acesso em: 28.11.2020.
[78] *Idem*.

este que figura como um dos fundamentos expressos da Lei Geral de Proteção de Dados Pessoais (LGPD)[79].

Extrai-se do acórdão notável influência do posicionamento do Tribunal Constitucional Federal Alemão[80], mencionado diversas vezes. Tal como no caso europeu, a corte brasileira tratar-se de uma deliberação de que "a proteção à autodeterminação informativa" se baseia no "direito fundamental da personalidade", entendendo, por sua vez, que o livre desenvolvimento da personalidade[81] pressupõe o poder individual de gerir seus dados pessoais[82]. Dessa forma, consignou-se que:

> Para garantir o direito de autodeterminação sobre a informação, também são necessárias precauções especiais no levantamento e processamento de dados, já que as informações, nessa fase, ainda são individualizáveis. Exige-se a estipulação de regras de eliminação para as informações auxiliares, como dados de identificação e que possibilitariam facilmente a quebra do anonimato, como nome, endereço, número de identificação e lista do recenseamento.

Além disso, argumentou-se que há violação à proporcionalidade ou proibição do excesso quando se buscam "restrições desproporcionais e arbitrárias ao direito à privacidade e ao sigilo das pessoas"[83]. Nessa toada, afirmou que "para a realização de uma pesquisa por amostra domiciliar não se faz necessário o acesso aos dados pessoais de todos os brasileiros, violando diversos sigilos, inclusive telefônicos". Dessa maneira, deve-se agir da maneira menos invasiva possível, o que na LGPD foi indicado, por exemplo, ao fixar-se o princípio da necessidade traduzido como "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". Deve-se, portanto, privilegiar sempre a menor limitação de direitos fundamentais[84].

A avaliação de outras possibilidades menos invasivas foi sublinha pelo STF, ao salientar-se no acórdão que "inexiste a extrema exigência de realização desta pesquisa estatística nesse momento de pandemia" e que "outro meio pode ser utilizado para a consecução do mesmo fim, tão logo haja a normalização da convivência social"[85].

---

[79] *Ibidem*.
[80] Bundesverfassungsgericht. **Urteil des Erten Senats vom 15**. Dezembro de 1983. Disponível em: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html>. Acesso em: 06.12.2020.
[81] PERLINGIERI, Pietro. **Perfis do Direito Civil.** Introdução ao Direito Civil Constitucional. 2. ed. Rio de Janeiro: Renovar, 2002. p. 158-159, § 103.
[82] Ação Direta de Inconstitucionalidade..., *Op. Cit*.
[83] *Idem*.
[84] DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos direitos fundamentais**. 5. ed. São Paulo: Atlas, 2014. p. 224.
[85] Ação Direta de Inconstitucionalidade..., *Op. Cit.*

A decisão do Supremo Tribunal Federal, sob a relatoria da Ministra Rosa Weber, evidenciou a "desnecessidade" e o "excesso do compartilhamento de dados" previsto na MP nº 954/2020, ao cotejá-los com a finalidade invocada pelo IBGE como sua justificativa, qual seja a realização do PNAD[86].

> O objetivo alegado não só pode, como está sendo realizado de forma menos intrusiva à privacidade. Assim, se a PNAD é realizada com uma amostra de pouco mais de duzentos mil domicílios, questiono: por que compartilhar duas centenas de milhões de números de telefone, com os riscos intrínsecos à manipulação desses dados? Somado tal fato ao adiamento do Censo 2020 para o próximo ano, parece-me que sua eloquência reverbera.

Além disso, entendeu a Corte que "não bastasse a coleta de dados se revelar excessiva", os dados coletados ainda seriam utilizados para a produção estatística oficial, o que permitiria a conservação dos dados pessoais, pelo ente público, por tempo "manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada"[87].

No que diz respeito à proporcionalidade da disponibilização dos dados:

> Destaco, ainda, que a desproporcionalidade no tocante ao universo dos dados a serem disponibilizados com base na MP nº 954/2020, em cotejo com as finalidades declaradas para o seu uso, se agrava pela ausência de previsão, no ato normativo, de cuidados mínimos para a sua anonimização ou pseudonimização, procedimentos técnicos pelos quais os dados perdem a capacidade de identificar, direta ou indiretamente, o indivíduo a que originalmente se refere, sendo certo que em momento algum a identificação dos indivíduos titulares dos dados foi reivindicada como necessária ao relevante trabalho desenvolvido pelo IBGE[88].

Ainda, ressalta que, apesar de prevista a exclusividade do uso dos dados coletados pelo IBGE, a medida provisória "não (contempla) garantia alguma que assegure o seu tratamento de forma segura"[89]. Com efeito, é preciso notar que a proporcionalidade se desdobra não apenas como critério de admissibilidade, mas deve também ser confrontada no plano protetivo. "Em síntese, quanto maior a invasão, maior deve ser a proteção"[90].

---

[86] PNAD – Pesquisa Nacional por Amostra de Domicílios.

[87] Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (COVID-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. BRASIL. Medida Provisória nº 954, de 17 de abril de 2020 (sem eficácia). Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1605035315518&disposition=inline>. Acesso em: 28 de novembro de 2020.

[88] STF. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Relª.: Minª. Rosa Weber.

[89] *Idem*.

[90] SCHULMAN, Gabriel. **Internação forçada, saúde mental e drogas:** é possível internar contra a vontade?. São Paulo: Foco, 2020.

No voto do Ministro Edson Fachin, como complementação à ideia aqui discutida, afirma-se que a MP intervém fortemente na esfera nuclear da configuração da vida privada. Segundo ele, "não se depreende que os protocolos de segurança no tratamento e no armazenamento de dados sigilosos tenham sido ampliados ou, simplesmente, aperfeiçoados na proporção da interferência que a MP causa aos direitos fundamentais dos usuários"[91]. Também nesse sentido, o Ministro Luís Barroso, em seu voto, afirma que "o compartilhamento de dados pessoais para fins de produção de estatísticas somente será compatível com o direito à privacidade", se:

> 1) a finalidade da pesquisa for precisamente delimitada;
> 2) o acesso for permitido na extensão mínima necessária para a realização dos seus objetivos;
> 3) forem adotados procedimentos de segurança suficientes para prevenir riscos de acesso desautorizado, vazamentos acidentais ou utilização indevida[92].

Em um olhar concreto sobre a necessidade, a proteção significa levar em conta um juízo sobre os riscos e impactos decorrentes de usos para finalidades distintas daquelas almejadas, expressas na justificação do IBGE. Como ressalta a ementa do acórdão, "deve ser anotado com um dado da realidade que, fragilizando o ambiente de proteção de dados pessoais no Brasil, obriga sejam medidas como a implementada na MP nº 954/2020 escrutinadas com maior cuidado, sob pena de se permitir que milhões de indivíduos sejam lesionados em suas esferas de direitos".

Assim, extrai-se da decisão que por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade devem ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com a manipulação de dados pessoais[93].

É de grande relevância, também, observar o controle estatal de seus próprios atos em matéria de proteção de dados pessoais. No caso em exame, a repercussão foi do Estado como solicitante e como gestor dos dados pessoais. É preciso, contudo, salientar que a proteção dos direitos fundamentais à luz da Constituição deve também abarcar outras duas "situações": a primeira consiste no Estado como titular de dados (por exemplo a localização de presos com tornozeleiras, CPF dos servidores públicos etc.); a segunda consiste no controle da própria atividade dos particulares. Atenta a tal perspectiva, a LGPD expressamente aponta Estado e particulares como destinatários de suas normas.

---

[91] STF. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Rel.: Minª. Rosa Weber.
[92] *Idem*.
[93] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, vol. 12, n. 2, p. 91-108, jul./dez. 2011.

3. A leitura da proteção de dados e da própria LGPD à luz da Constituição

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) estabelece, reitera e enfatiza um importante acervo de direitos e princípios para o tratamento de dados pessoais. Em seu núcleo, a LGPD estabelece condições de legitimidade para o tratamento de dados pessoais, com hipóteses legais em que violada, por óbvio, redunda na ilegalidade do uso dos dados. Por meio da legislação, confere-se ampla proteção à pessoa concreta, nas relações entre particulares e com o Estado, consagrando a autodeterminação informativa[94] durante todo o ciclo de dados pessoais. Suas normas dialogam com a concretização da dignidade da pessoa humana, livre desenvolvimento da personalidade, cidadania, direitos humanos e fundamentais. Dessa maneira, trata-se de norma que estabelece interessantes parâmetros para a efetivação do direito fundamental à proteção de dados, reconhecido pelo STF em seu acórdão[95].

Além de reconhecer o caráter constitucional da proteção de dados pessoais, Mulholland[96] sublinha que uma primeira análise da estrutura constitucional dos direitos fundamentais leva ao reconhecimento de que a proteção de dados pessoais, ainda que não prevista constitucionalmente de forma expressa, poderia ser tutelada em relação à proteção da intimidade, ao direito à informação, direito ao sigilo de comunicações e dados, e a garantia individual ao conhecimento e correção de informações sobre si pelo *habeas corpus*[97]. Proteger os dados pessoais se torna, então, instrumento para a efetivação de (outros) direitos fundamentais.

Rodotà sustenta que a proteção de dados corresponde a um verdadeiro direito fundamental autônomo, pressuposto da cidadania, expressão da liberdade e da dignidade

[94] FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana. TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2019. p. 100.

[95] O acórdão menciona também o reconhecimento pela Corte Alemã e em julgado do "Tribunal de Justiça da União Europeia num caso exatamente de Digital Rights Ireland".

[96] Interessante ressaltar que, enquanto o presente capítulo busca apresentar uma leitura da Lei Geral de Proteção de Dados à luz do texto constitucional, Mulholland percorre o caminho inverso, realizando uma leitura funcionalizada da Constituição Federal e de seus princípios e valores, considerando a tutela da privacidade como *locus* constitucional da proteção dos dados pessoais. As duas leituras, correlatas e complementares, enfatizam a necessária aplicação da metodologia da constitucionalização da interpretação dos instrumentos legislativos.

[97] MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direito e Garantias Fundamentais**, Vitória, vol. 19, n. 3, p. 159-180, set./dez. 2018. p. 171.

humana, que está intrinsicamente relacionada à impossibilidade de transformar as pessoas em objeto de vigilância constante[98].

> [...] estamos diante da verdadeira reinvenção da proteção de dados – não somente porque ela é expressamente considerada como um direito fundamental autônomo, mas também porque se tornou uma ferramenta essencial para o livre desenvolvimento da personalidade. A proteção de dados pode ser vista como a soma de um conjunto de direitos que configuram a cidadania do novo milênio[99].

No mesmo compasso, Frazão aponta que a LGPD pode, igualmente, ser vista como um freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância[100], a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas sem a ciência ou o consentimento informado dos usuários[101]. A entrada em vigor de um estatuto claramente voltado à tutela de uma situação em que há particular vulnerabilidade, nomeadamente diante dos riscos conhecidos e desconhecidos das "novas" tecnologias, suscita reflexões sobre o juízo valorativo efetuado pelo legislador ao atribuir expressamente certos direitos ao grupo vulnerável – os titulares de dados pessoais[102].

Por força da perspectiva dos princípios constitucionais da prevenção e precaução, assim como em vista dos princípios do livre acesso, segurança e prevenção da LGPD (art. 6º, incs. V, VII, VIII), deve-se consagrar a confidencialidade, integridade e disponibilidade. A confidencialidade significa assegurar que uma informação não seja disponibilizada ou exposta. A necessidade de se manter intacta a informação (ela deve circular sem sofrer alterações, ou seja, permanecer protegida mesmo que se compartilhada); e ao fato de que a informação pode ser obtida, se for necessária (pode-se obter uma informação, ainda que confidencial)[103].

Nas palavras da Relatora Min. Rosa Weber ao julgar o caso do Censo:

---

[98] RODOTÀ, Stefano. **A vida na sociedade de vigilância. A privacidade hoje**. Rio de Janeiro: Renovar, 2008. p. 18-19.
[99] RODOTÀ. *Op. Cit.*, p. 14.
[100] Sobre a expressão, cf. ZUBOFF, Shoshana, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, **Journal of Information Technology,** v. 30, p. 75–89. April 4, 2015.
[101] FRAZÃO, Ana. Fundamentos para a proteção dos dados pessoais. Noções introdutórias para a compreensão da LGPD. In: FRAZÃO, Ana. TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2019.
[102] SOUZA, Eduardo Nunes. SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. **Pensar Revista de Ciências Jurídicas**, Fortaleza, vol. 4, n. 3, p. 1-22, jul./set. 2019. p. 2.
[103] "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability". NIELES, Michael; DEMPSEY, Kelley; PILLITTERI, Victoria Yan. **An Introduction to Information Security**. IST Special Publication 800-12 Revision 1.

> ao não prever exigência alguma quanto a mecanismos e procedimentos para assegurar o sigilo, a higidez e, quando o caso, o anonimato dos dados compartilhados, a MP n. 954/2020 não satisfaz as exigências que exsurgem do texto constitucional no tocante à efetiva proteção de direitos fundamentais dos brasileiros[104].

Em interessante leitura das ideias de Daniel Solove[105], o acórdão ressalta um movimento pendular pela qual se procura, frequentemente, propor uma dicotomia entre privacidade e segurança, rechaçada pelo STF. A legitimidade do tratamento de dados pessoais leva em conta não apenas sua finalidade, mas também a proteção. Dessa maneira, sem negar a importância do Censo, a rejeição da MP levou-se em conta que "o imediato compartilhamento de dados pode causar danos irreparáveis à intimidade".

Além disso, e no que se relaciona à temática discutida pela ADI nº 6.387, a LGPD apresenta uma disciplina jurídica que estabelece deveres, no âmbito da proteção de dados pessoais, também em relação à administração pública. O texto da LGPD regulamenta de maneira específica tratamento de dados pessoais pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres[106], observadas as disposições do Capítulo IV da lei. As políticas em questão podem envolver, por exemplo, a implementação de saneamento básico, de auxílios a cidadãos em situação de vulnerabilidade ou de projetos voltados à educação de crianças e adolescentes[107].

A execução de políticas públicas é também uma das justificativas para que o setor público realize tratamento de dados. Nesse sentido, vale ressaltar que a LGPD estabelece critérios para o tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas pela Lei de Acesso à Informação (Lei nº 12.527/2011)[108], devendo ser realizado

---

[104] STF. **Medida Cautelar na Ação Direta de Insconstitucionalidade n.º 6.387.** Rel: Ministra Rosa Weber.

[105] SOLOVE, Daniel J. **Nothing to hide**: The false tradeoff between privacy and security. Yale University Press, 2011.

[106] Art. 5º, XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;

[107] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilística.com**, Rio de Janeiro, ano 9, n. 1, 2020, p. 1-38. p. 22.

[108] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
Parágrafo único. Subordinam-se ao regime desta Lei:

para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público[109]. Todo o exposto pode ocorrer desde que contempladas duas condições[110]. A primeira, que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos. E a outra, que seja indicado um encarregado quando realizarem operações de tratamentos de dados pessoais.

Percebe-se, assim, que a LGPD é um importante passo rumo ao fortalecimento do marco normativo da sociedade da informação no Brasil[111], estimulando o desenvolvimento de uma cultura de proteção de dados, a construção de uma estrutura institucional para a aplicação da lei, e também o incentivo à aplicação conjunta de normas e princípios já existentes no ordenamento brasileiro. Há também uma preocupação em relação aos diversos atores inseridos nesse contexto de discussão, e também na dinâmica de problemáticas atuais, como o posicionamento e enfrentamento de dados pela administração pública em relação à pandemia de COVID-19.

Nesse sentido, a essência constitucional que orienta (e deve orientar) a legislação é muito importante, uma vez que reafirma a natureza de direito fundamental da autodeterminação informativa e da própria proteção de dados pessoais. A lei regulamenta e complementa, de modo geral, a legislação que se correlaciona à temática[112], ressaltando **o exame da proporcionalidade como parte do processo de proteção dos direitos fundamentais**. O eixo valorativo da LGPD é a proteção da pessoa humana e de suas situações existenciais relevantes, o que, em conjunto com a Constituição e os princípios constitucionais que iluminam a legislação, deve ser levado em consideração para a interpretação de suas disposições.

I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

[109] Art. 23, da Lei Geral de Proteção de Dados Pessoais.

[110] Art. 23, I e II, da Lei Geral de Proteção de Dados Pessoais.

[111] MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, vol. 120, ano 27, nov./dez. 2018, p. 469-483. p. 482.

[112] Das quais podem ser citadas, entre tantas outras: Código Civil, Marco Civil da Internet e Código de Defesa do Consumidor, Lei de Acesso à Informação.

Exige-se na atividade de interpretação, a aplicação de um itinerário interpretativo denso, iluminado pelos preceitos constitucionais, cujas etapas perpassam inclusive o indispensável cotejo crítico entre direito e concretude, de modo a promover a tutela da pessoa humana, em sintonia com a constitucionalização de todo direito.

4. (Re)Significação da proteção de dados e a legalidade constitucional

A decisão proferida pelo STF ao julgar a inconstitucionalidade da MP n. 954/2020, a partir do exame da proporcionalidade, identificou excessos no tratamento de dados pessoais e, por conseguinte, sua contrariedade à legalidade constitucional. A compreensão foi corroborada pela legislação e, também, por agências reguladoras, que destacam a necessária observância de extrema cautela no tratamento dos dados de usuários de serviços de telecomunicações, por exemplo. Destaca-se a necessidade de se assegurar a proteção da privacidade, da intimidade e dos dados pessoais, e de diversos princípios expostos na LGPD. Para ilustrar, se a pesquisa do Censo é feita por amostragem, porque é necessário ter acesso a todos os dados e dados de todos? Ademais, porque a MP estipulava prazos exíguos como três dias para o presidente do IBGE regulamentar o "procedimento para a disponibilização dos dados" (MP n. 954/2020, art. 2º, § 2º) e o recebimento de todo o acervo de dados nos sete dias subsequentes (MP n. 954/2020, art. 2º, § 3º, inc. I)?

A Lei Geral de Proteção de Dados Pessoais reforça a importância da delimitação específica da *finalidade do uso dos dados* já consagrada pelo texto constitucional. Note-se que o texto da MP aponta uma finalidade muito genérica ("estatística oficial"), não estabelece padrões de segurança, não justifica para que pedir o telefone, não esclarece por que exigir dados, também de pessoa jurídicas. Também não havia mecanismos de controle que permitissem aferir o uso subsequente, ou seja, a pertinência[113] ao propósito inicial. Embora haja previsão de eliminação os dados após o fim do estado de emergência, faltam elementos que permitam *accountability.*

Nessa toada, importante notar que o princípio da finalidade estabelece que os fins para os quais os dados pessoais serão utilizados devem estar especificados no momento de sua coleta, e que seu uso subsequente seja compatível com o propósito inicial, de modo

[113] MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Facebook como o novo *big brother*: uma abertura para a responsabilização civil por violação à autodeterminação informativa. **Quaestio Iuris,** Rio de Janeiro, vol. 10, nº 04, 2017, p. 2319-2338.

a efetivar o princípio da pertinência[114]. Assim, defende-se o entendimento de que o tratamento dos dados pessoais só deve ser realizado quando necessário ao atendimento da finalidade concedida, devendo ocorrer de modo mais simplificado possível, sem que se legitime a utilização desproporcional desses dados[115].

Ao reiterar o texto constitucional que consagra a adequação entre meios e fins, a legislação federal além de regulamentar repete os valores constitucionais, encorpando a reverberação das normas constitucionais. *Em oposição a tais premissas,* como detalha-se no julgamento, a MP não delimitou o "objeto da estatística a ser produzida, nem a finalidade específica, tampouco a amplitude"[116]. Igualmente não esclarece a necessidade de disponibilização dos dados nem como serão efetivamente utilizados. Nessa toada, é necessário ressaltar que os princípios da LGPD são guias úteis e necessários para a proteção de dados pessoas e, inclusive, para estabelecer uma boa governança de dados.

Questionar critérios, parâmetros e espaços de proteção é, portanto, parte relevante do processo de reflexão e (re)significação da proteção de dados pessoais[117]. Trata-se de ingredientes relevantes que tornam ainda mais complexas as análises em torno da proteção de dados pessoais e, também, da própria privacidade[118]. A proporcionalidade, prevenção, precaução, segurança, transparência não são normas jurídicas "apenas" da LGPD, mas do ordenamento brasileiro, e de grande utilidade para solucionar questões em matéria de proteção de dados pessoais[119].

Na medida em que a informação se impõe como instrumento de distribuição de riquezas e combustível do progresso econômico, não deve ser legítima sua utilização de forma ilimitada[120], sob o risco de ferir de valores e princípios para a ordem jurídica, cabendo ao Direito estabelecer limites para sua utilização, de modo a impedir que o manejo desse bem econômico venha a violar quaisquer direitos, notadamente os direitos de personalidade.

A discussão aqui trazida permite revelar, desta maneira, a necessária conexão entre a proteção e utilização de dados com os valores constitucionais. A proteção de dados

---

[114] *Idem*.
[115] *Ibidem*.
[116] Supremo Tribunal Federal (STF). **Medida Cautelar na Ação Direta de Insconstitucionalidade n.º 6.387.** Rel: Ministra Rosa Weber.
[117] SCHULMAN, Gabriel; SCHIRRU, Luca. Pequenos titulares e grandes desafios, a proteção de dados pessoais de crianças e adolescentes: um debate sobre melhor interesse, (des)equilíbrios, e LGPD a partir do episódio "*arkangel*" da série "*black mirror*". **Revista da Ouvidoria**, Tribunal de Justiça do Estado do Paraná, 2ª edição, 2020, p. 27-51. p. 32.
[118] *Idem*.
[119] SCHULMAN; SCHIRRU, *Op. Cit*., p. 33.
[120] MENEZES; COLAÇO, *Op. Cit*., p. 2325.

pessoais no ordenamento brasileiro não se estrutura a partir de um diploma legal isolado A Constituição Brasileira contempla o problema da informação inicialmente por meio das garantias à liberdade de expressão e do direito à informação, que deverão eventualmente ser confrontados com a proteção da personalidade e, em especial, com o direito à privacidade[121]. Também protege sigilo, intimidade, dignidade e livre desenvolvimento.

A própria designação da LGPD como uma "lei geral" deve ser bem compreendida. Defendê-la como uma ilha, tal como se fazia no oitocentos em relação ao código civil é linha de pensamento que não coaduna nem ao mesmo com o próprio texto legislativo. A opção pelo argumento legalista na compreensão a LGPD – seja no sentido de se buscar um local obscuro, longe da leitura à luz da constituição, seja no sentido de aplicar a LGPD como uma norma autossuficiente colide com a própria leitura do teor da lei. No texto normativo, consta a previsão de que devem ser consideradas normas "gerais e setoriais" (LGPD, art. 34, inc. I), além disso, determina-se que a ANPD deve articular-se com as "autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação" (LGPD, art. 55-J, inc. XXIII). Há previsão também de diálogo com o Código de Defesa do Consumidor, com expressa previsão de que as sanções ali previstas persistem (LGPD, art. 52, § 2º). A incidência da Constituição não depende – e nem pode ser condicionada – pela legislação infraconstitucional. Não obstante, há expressa na LGPD, art. 55-J, § 1º, há expressa previsão da incidência dos princípios do art. 170, da CF, que incluem, vale lembrar, a proteção do consumidor.

Há, portanto, um desafio de interpretação que compreende a LGPD como mais uma norma do nosso ordenamento que precisa ser conjugada. Seu sentido geral se traduz assim em uma eficácia irradiante, não em seu isolamento.

Essa percepção também é útil para que o argumento da absoluta novidade da LGPD não seja tomado como a ignorar toda a construção jurídica em torno de vários dos princípios que traz, ou melhor, que repete de outras normas. Trata-se de uma lei positiva, que apresenta e reforça muitas temáticas já legisladas de forma esparsa. Apesar de ter visibilizado o tema da proteção de dados pessoais, é necessário que não se esqueça dos outros diplomas, especialmente da Constituição Federal.

[121] DONEDA, *Op. Cit*., p. 103.

5. "O caminho se faz no andar": Aprendizados úteis e considerações finais

> As restrições deste direito à "autodeterminação sobre a informação" são permitidas somente em caso de interesse predominante da coletividade. Tais restrições necessitam de uma base legal constitucional que deve atender ao mandamento da clareza normativa próprio do Estado de Direito. O legislador deve, além disso, observar, em sua regulamentação, o princípio da proporcionalidade. Também deve tomar precauções organizacionais e processuais que evitem o risco de uma violação do direito da personalidade[122].

O julgamento do Caso do Censo do IBGE pelo STF permite importantes lições, as quais em diversos pontos permitem aproveitar as conclusões da Corte Alemã. De maneira sistemática, entre outras contribuições úteis que se pode obter do exame do julgamento da ADI n. 6387 pelo Supremo Tribunal Federal, cumpre salientar, sob o prisma da legalidade constitucional:

- **i.** reconhecimento da autodeterminação informativa e da proteção de dados pessoais como direitos fundamentais autônomos;
- **ii.** aplicação da proporcionalidade em matéria de proteção de dados pessoais, parâmetro que permeou o exame da finalidade do uso dos dados pessoais, do grau de invasão na esfera pessoas, na apreciação no risco e na avaliação da (in)suficiência das proteções oferecidas no tratamento de dados pessoais;
- **iii.** à luz de uma leitura constitucional, impõe-se uma avaliação a priori dos riscos, à luz do binômino probabilidade e consequências, o que exige o devido esclarecimento, inclusive com base na garantia do devido processo legal;
- **iv.** não há dados pessoais neutros ou insignificantes, sobretudo porque em uma análise contextual a associação de dados ou processamentos eletrônicos podem implicar consequências muito danosas[123].
- **v.** é preciso confrontar riscos e mecanismos protetivos de maneira concreta;
- **vi.** a falta de relatório de impacto opõe-se à perspectiva protetiva que orienta a materialização do direito fundamental à proteção de dados pessoais;
- **vii.** deve-se analisar a possibilidade de identificação das pessoas, e o impacto desta identificação[124];
- **viii.** o sigilo, intimidade e privacidade não são direitos absolutos; por outro lado, sua flexibilização é excepcional e deve ser fundamentada;
- **ix.** faz-se necessário um repensar da proteção dos dados pessoais diante do advento de novos mecanismos tecnológicos.

---

[122] Trata-se de trecho da fundamentação do conhecimento julgamento da Lei do Censo pelo Tribunal Constitucional alemão. SCHWABE, Jürgen. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Uruguai: Konrad Adenauer-Stiftung, 2005. p. 235.

[123] SCHWABE, *Op. cit*. p. 239. Extrai-se do acórdão da Lei do Censo: "Decisivos são sua utilidade e possibilidade de uso. Estas dependem, por um lado, da finalidade a que serve a estatística e, por outro lado, das possibilidades de ligação e processamento próprias da tecnologia de informação. Com isso, um dado em si insignificante pode adquirir um novo valor: desse modo, não existem mais dados "insignificantes" no contexto do processamento eletrônico de dados".

[124] Extrai-se do acórdão: "há o risco de identificação precisa e formação de perfil dos usuários. Dados como nome, endereço e telefone de todos os usuários dos serviços de telefonia móvel e fixa, somados às entrevistas
pessoais, podem gerar um nível preocupante de precisão na identificação dos usuários".

A teor do acórdão, a aplicação da LGPD ocorreu como mecanismo de controle do próprio ente estatal, a demonstrar os enormes riscos que envolvem a matéria de dados pessoais. A respeito, ao argumento de que o censo é relevante deve-se contrapor a própria credibilidade do Estado e do IBGE. Não deixa de ser curioso recordar que, em 2017, foi o próprio IBGE que argumentava a proteção ao sigilo estatístico para rejeitar pedido do Ministério Público Federal que pretendia compelir o instituto "a prestar informações necessárias à identificação de 45 crianças domiciliadas em Bauru/SP que, de acordo com o censo realizado em 2010, não teriam sido regularmente registradas nos Cartórios de Registro Civil de Pessoas Naturais"[125]. Na ocasião, o STF ao assegurar a proteção do sigilo, destacou que "o afastamento excepcional do sigilo estatístico, surge como grave precedente e parece ganhar contornos extravagantes"[126].

No tocante ao ciclo dos dados pessoais, além de não haver mecanismos de controle, a avaliação do risco seria feita após já ter ocorrido a coleta, em oposição à ótica preventiva e proativa que orienta a LGPD. "Ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP nº 954/2020 desatende a garantia do devido processo legal (art. 5º, LIV, da CF)"[127]. Nessa linha, constava da MP, em seu art. 2º, "A Fundação IBGE informará, em seu sítio eletrônico, as situações em que os dados referidos no caput do art. 2º foram utilizados e divulgará relatório de impacto à proteção de dados pessoais"[128].

Falha-se também por não ter se definido uma estratégia de redução do tempo de exposição dos dados pessoais afinal, se não houver como alcançar um resultado sem a utilização de dados pessoais, estes devem ser eliminados o quanto antes. Em relação ao ciclo dos dados pessoais, de forma igualmente vaga se estabelecia no art. 4º da MP que "Superada a situação de emergência de saúde pública" as informações coletadas "serão eliminadas das bases de dados da Fundação IBGE"[129]. Embora houvesse na MP previsão de exclusão dos dados pessoais após o fim do estado de emergência, não foram definidos mecanismos de controle que que permitissem acompanhar o cumprimento dessa promessa, gerir, e comprová-la quanto executada.

---

[125] STF. **SL 1103**. Rel.: Minª. CÁRMEN LÚCIA. DJE: 05.05.2017.
[126] STF. **ADI n. 6387**. Relª. Minª. Rosa Weber. Tribunal pleno. Dje: 11.11.2020.
[127] *Idem*.
[128] BRASIL. **Medida Provisória nº 954**, de 17 de abril de 2020 (sem eficácia). Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1605035315518&disposition=inline>
[129] BRASIL. **Medida Provisória nº 954**, de 17 de abril de 2020 (sem eficácia). Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1605035315518&disposition=inline>.

A proteção de dados pessoais impõe que haja mecanismos para controlar e comprovar tal medida, em sintonia com a *accountability*[130] *estabelecida pela LGPD em muitas passagens (art. 6º, inc. X; art. 32, art. 37, art. 38, entre outros), assim como decorrência do direito fundamental à proteção de dados pessoais e do direito fundamental autodeterminação informativa, em harmonia com os princípios da publicidade, legalidade, transparência que orientam a Administração Pública (CR, art. 37), bem como a proteção da dignidade humana, inviolabilidade da intimidade, da privacidade e da vida privada, sigilo de dados (CR, art. 1º, 5º, caput e inc. X).*

Nessa toada, é necessário ressaltar que os princípios da Lei Geral de Proteção de Dados Pessoais são guias úteis e necessários para a proteção de dados pessoas e, inclusive, para estabelecer uma boa governança de dados. Questionar critérios, parâmetros e espaços de proteção é, portanto, parte relevante do processo de reflexão e (re)significação da proteção de dados pessoais[131]. Trata-se de ingredientes relevantes que tornam ainda mais complexas as análises em torno da proteção de dados pessoais e, também, da própria privacidade[132].

A proporcionalidade, prevenção, precaução, segurança, transparência não são normas jurídicas "apenas" da LGPD, mas do ordenamento brasileiro, e de grande utilidade para solucionar questões em matéria de proteção de dados pessoais[133]. Não deixa de ser significativa, nessa linha, a própria circunstância de que o STF aplicou a LGPD antes mesmo de sua vigência.

Apenas para rápidos exemplos sobre a presença nos princípios antes e independente da LGPD, a precaução e prevenção não são princípios novos, são empregados há anos em matéria ambiental; transparência e informação adequada nas relações Estado-cidadão e no âmbito das relações de consumo são igualmente conhecidos.

É notável a circunstância de terem sido empregados antes da vigência da lei, o que decorre do fato de serem princípios jurídicos anteriores a LGPD, porém, também, da consagração da própria constitucionalidade do diploma legal. Na medida em que a informação se impõe como instrumento central da economia, não deve ser legítima sua

[130] **The Privacy, Data Protection and Cybersecurity Law Review.** Alan Charles Raul (Editor). 3. ed. Reino Unido: Law Business Research Ltd, 2016. p. 15.
[131] SCHULMAN, Gabriel; SCHIRRU, Luca. Pequenos titulares e grandes desafios, a proteção de dados pessoais de crianças e adolescentes: um debate sobre melhor interesse, (des)equilíbrios, e LGPD a partir do episódio "*arkangel*" da série "*black mirror*". **Revista da Ouvidoria**, Tribunal de Justiça do Estado do Paraná, 2ª edição, 2020, p. 27-51. p. 32.
[132] *Idem*.
[133] SCHULMAN; SCHIRRU, *Op. Cit*., p. 33.

utilização de forma ilimitada[134], sob o risco de ferir de valores e princípios para a ordem jurídica. Deve, portanto, submeter-se a legalidade constitucional.

A opção pelo argumento legalista na compreensão a LGPD – seja no sentido de se buscar um local obscuro longe da leitura à luz da constituição, seja no sentido de aplicar a LGPD como uma norma autossuficiente colide com a própria leitura do teor da lei. No texto normativo, consta a previsão de que devem ser consideradas normas "gerais e setoriais" (LGPD, art. 34, inc. I), além disso, determina-se que a ANPD deve articular-se com as "autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação" (LGPD, art. 55-J, inc. XXIII). Há previsão também de diálogo com o Código de Defesa do Consumidor, com expressa previsão de que as sanções ali previstas persistem (LGPD, art. 52, § 2º). A incidência da Constituição não depende – e nem pode ser condicionada – pela legislação infraconstitucional. Não obstante, há expressa na LGPD, art. 55-J, § 1º, há expressa previsão da incidência dos princípios do art. 170, da CF, que incluem, vale lembrar, a proteção do consumidor.

Há, portanto, um desafio de interpretação que compreende a LGPD como mais uma norma do nosso ordenamento cuja unidade e complexidade já restou acima exposta. Seu sentido geral se traduz assim em uma eficácia irradiante, não em seu isolamento. Essa percepção também é útil para que o argumento da absoluta novidade da LGPD não seja tomado como a ignorar toda a construção jurídica em torno de vários dos princípios que traz, ou melhor, que repete de outras normas. Também permite melhor aproveitar o desenvolvimento doutrinário e jurisprudencial em torno da proteção da vida privada, do sigilo, da intimidade.

Por fim, é importante frisar que a LGPD é uma ferramenta com enorme potencial, desde que bem empregada. Propõe-se aqui sua análise com a perspectiva *fractal*: deve-se olhar de perto e de longe para compreender sua complexidade. Em outras palavras, aproximações e distanciamentos, a partir do necessário diálogo com outros instrumentos regulatórios, como o Marco Civil da Internet, mas, especialmente, com o texto constitucional e seus reflexos na compreensão e interpretação da legislação.

O advento de novas tecnologias potencializa as possibilidades de uso de dados. A teor do acórdão que julgou a ADI n. *6387*, "quanto maior for a capacidade de acumulação

[134] MENEZES; COLAÇO, *Op. Cit*., p. 2325.

e armazenamento da informação, maior a potencialidade de que elas possam ser elemento fundamental de influência em nosso cotidiano"[135].

Como no verso de Antonio Machado, tomado por empréstito no título desta seção, "El camino se hace al andar"[136]. A legalidade constitucional demanda uma construção dinâmica de sentidos das normas, apta a captar as novas tecnologias. É preciso, dessa maneira, conferir flexibilidade ao sistema jurídico[137] e porosidade à realidade concreta. Como apontou o voto do Min. Gilmar Mendes, "nunca foi estranha à jurisdição constitucional a ideia de que os parâmetros de proteção dos direitos fundamentais devem ser permanentemente abertos à evolução tecnológica"[138]. Por fim, seu voto acrescenta outra advertência, que consiste em apreender um sentido mais amplo a proteção de dados, porque "a disciplina jurídica do processamento e da utilização da informação acaba por afetar o sistema de proteção de garantias individuais como um todo"[139].

6. Referências bibliográficas

ALEXY, Robert. **Teoria dos direitos fundamentais**. São Paulo: Malheiros, 2008.

ÁVILA. Humberto. **Teoria dos Princípios**. Da definição à aplicação dos princípios jurídicos. 4. ed. São Paulo: Malheiros, 2005.

BARBOZA, Heloísa Helena. Reflexões sobre autonomia negocial. In: TEPEDINO, Gustavo, FACHIN, Luiz Edson (coord.). **O direito e o tempo**: embates jurídicos e utopias contemporâneas – Estudos em homenagem ao Professor Ricardo Pereira Lira. Rio de Janeiro: Renovar, 2008.

BARBOZA, Heloisa Helena. Vulnerabilidade e cuidado: aspectos jurídicos. In: PEREIRA, Tânia; OLIVEIRA, Guilherme de (coord.). **Cuidado e vulnerabilidade.** São Paulo: Atlas, 2009, p. 106-118.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**. **A construção de um conceito jurídico à luz da jurisprudência mundial**. Belo Horizonte: Fórum, 2014.

BARROSO, Luís Roberto. **Curso de Direito Constitucional Contemporâneo**. Os conceitos fundamentais e a construção do novo modelo. 9. ed. Saraiva, 2019.

[135] STF. **Medida Cautelar na Ação Direta de Insconstitucionalidade n.º 6.387.** Rel: Ministra Rosa Weber.
[136] MACHADO, Antonio. **Poesías Completas**. México: Universidad Autónoma del Estado de México, 2016. p. 87.
[137] ZAGREBELSKY. **El Derecho Dúctil. Ley, Derecho, Justicia**. 8. ed. Madrid (Espanha): Editorial Trotta, 2008.
[138] STF. **Medida Cautelar na Ação Direta de Insconstitucionalidade n.º 6.387.** Rel: Ministra Rosa Weber.
[139] *Idem*.

BARROSO, Luís Roberto. Fundamentos Teóricos e Filosóficos do Novo Direito Constitucional Brasileiro. **Revista da EMERJ**, vol. 4, n. 15, 2001, p. 1-47.

BODIN DE MORAES, Maria Celina. A Caminho de um Direito Civil Constitucional. **Revista de Direito Civil Imobiliário, Agrário e Empresarial**, São Paulo, vol. 65, ano 17, jul./set. 1993, p. 21-32.

BODIN DE MORAES, Maria Celina. Do juiz boca-da-lei à lei segundo a boca-do juiz: notas sobre a aplicação-interpretação do direito no início do Século XXI. **Revista de Direito Privado**, São Paulo, ano 14, vol. 56, p.11-30, out./dez. 2013.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020 (sem eficácia). Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8097182&ts=1605035315518&disposition=inline>. Acesso em: 28 de novembro de 2020.

Bundesverfassungsgericht. **Urteil des Erten Senats vom 15**. Dezembro de 1983. Disponível em: <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html>. Acesso em: 06.12.2020.

CANARIS, Claus-Wilhelm. A influência dos direitos fundamentais sobre o direito privado na Alemanha. In: SARLET, Ingo Wolfgang (Org.). **Constituição, Direitos Fundamentais e Direito Privado.** 2. ed. Porto Alegre: Livraria do Advogado, 2006. p. 225-245.

CANARIS, Claus-Wilhelm. **Direitos Fundamentais e Direito Privado.** Coimbra (Portugal): Almedina, 2006.

DIMOULIS, Dimitri; MARTINS, Leonardo. **Teoria geral dos direitos fundamentais**. 5. ed. São Paulo: Atlas, 2014.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, vol. 12, n. 2, p. 91-108, jul./dez. 2011.

FACHIN, Luiz Edson (Coord.). **Repensando fundamentos de Direito Civil Brasileiro Contemporâneo.** Rio de Janeiro: Renovar, 1998.

FACHIN, Luiz Edson. **Direito Civil. Sentidos, transformações e fim.** Rio de Janeiro: Renovar, 2015.

FLÓREZ-VALDÉS, Joaquín Arce y. **El derecho civil constitucional**. Madrid (Espanha): Civitas, 1991.

FRAZÃO, Ana. Fundamentos para a proteção dos dados pessoais. Noções introdutórias para a compreensão da LGPD. In: FRAZÃO, Ana. TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais. 2019.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: FRAZÃO, Ana. TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). **A Lei Geral de Proteção de Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos

Tribunais. 2019. p. 100.

GROSSI, Paolo. A formação do jurista e a exigência de um hodierno "repensamento" epistemológico. (Trad. Ricardo Marcelo Fonseca). **Revista da Faculdade de Direito da UFPR,** Curitiba, UFPR, v. 40, p .6-25, 2004.

HERRERA FLORES, Joaquín. ¿Crisis de la ideología o ideología de la crisis? Respuestas neoconservadoras. Crítica Jurídica, **Revista Latino Americana de Política, Filosofía y Derecho**, UNAM/Instituto de Investigaciones Jurídicas, n. 13, p. 123-143, 1993.

HESSE, Konrad. **Força Normativa da Constituição**. Porto Alegre: Sergio Fabris, 1991.

IBGE. **Comunicado sobre adoção da Medida Provisória 954/2020**. Disponível em: <https://www.ibge.gov.br/novo-portal-destaques/27477-comunicado-sobre-adocao-da-medida-provisoria-954-2020.html>. Acesso em 05.11.2020.

LÔBO, Paulo Luiz Netto. Constitucionalização do direito civil. **Revista de Informação Legislativa.** Brasília, Senado Federal, n. 141, ano 36, p. 99-109, jan./mar. 1999.

MACHADO, Antonio. **Poesías Completas**. México: Universidad Autónoma del Estado de México, 2016.

MANGUEIRA. **História pra ninar gente grande. Samba enredo de 2019**. Disponível em: <https://g1.globo.com/rj/rio-de-janeiro/carnaval/2019/noticia/2019/01/19/mangueira-veja-a-letra-do-samba-enredo-do-carnaval-2019-no-rj.ghtml>. Acesso em 05.11.2020.

MENDES, Laura Schertel. Habeas Data e autodeterminação informativa: dois lados da mesma moeda. ***Revista Direitos Fundamentais & Justiça,*** a. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, vol. 120, ano 27, nov./dez. 2018, p. 469-483.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Facebook como o novo *big brother*: uma abertura para a responsabilização civil por violação à autodeterminação informativa. **Quaestio Iuris,** Rio de Janeiro, vol. 10, nº 04, 2017, p. 2319-2338.

MORAES, Maria Celina Bodin de. O conceito de dignidade humana. In: _____. **Princípios do direito civil contemporâneo**. Rio de Janeiro: Renovar, 2006. p. 1-60.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). **Revista de Direito e Garantias Fundamentais**, Vitória, vol. 19, n. 3, p. 159-180, set./dez. 2018.

NEVES, Maria do Céu Patrão. Sentidos da vulnerabilidade: característica, condição, princípio. **Revista Brasileira de Bioética***, v.* 2. n. 02, p. 153-172, 2006.

NIELES, Michael; DEMPSEY, Kelley; PILLITTERI, Victoria Yan. **An Introduction to Information Security**. IST Special Publication 800-12 Revision 1.

NOVAIS, Jorge Reis. **A dignidade da pessoa humana. Dignidade e direitos fundamentais**. v. I, Coimbra: Almedina, 2015.

PERLINGIERI, Giovanni. **Profili applicativi della ragionevolezza nel diritto civile**. Napoli: Edizioni Scientifiche Italiane, 2015.

PERLINGIERI, Pietro. **La dottrina del diritto civile nella legalità costituzionale**. Conferência Magna proferida por ocasião do Congresso de Direito Civil Constitucional da Cidade do Rio de Janeiro. Rio de Janeiro: 21/09/2006.

PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional.** Rio de Janeiro: Renovar, 2008.

PERLINGIERI, Pietro. **Perfis do Direito Civil. Introdução ao Direito Civil Constitucional.** 2. ed. São Paulo: Renovar, 2002.

RAMOS, Carmem Lucia Silveira. Constitucionalização do direito privado e a sociedade sem fronteiras. In: FACHIN, Luiz Edson (Coord.). **Repensando fundamentos de Direito Civil Brasileiro Contemporâneo.** Rio de Janeiro: Renovar, 1998. p. 3-29.

RODOTÀ, Stefano. **A vida na sociedade de vigilância. A privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **La vita e le regole**. Tra diritto e non diritto. 4. ed. Milão: Feltrini, 2007.

SANCHÍS, Luis Pietro. **Constitucionalismo y Positivismo.** 2. ed. México: Fontamara, 1999. (Biblioteca de Ética Filosofía del Derecho y Política, v. 60).

SARMENTO, Daniel. Os Princípios Constitucionais e a Ponderação de Bens. *In:* TORRES, Ricardo Lobo. (Org.). **Teoria dos Direitos Fundamentais**. Rio de Janeiro: Renovar, 1999. p. 35-93.

SCHIER, Paulo Ricardo. **Filtragem Constitucional.** Construindo uma nova dogmática jurídica. Porto Alegre: Sergio Antonio Fabris, 1999.

SCHREIBER, Anderson; KONDER, Carlos Nelson. Uma agenda para o direito civil-constitucional. **Revista Brasileira de Direito Civil**, vol. 10, out./dez. 2016.

SCHULMAN, Gabriel. **Internação forçada, saúde mental e drogas:** é possível internar contra a vontade? São Paulo: Foco, 2020.

SCHULMAN, Gabriel; SCHIRRU, Luca. Pequenos titulares e grandes desafios, a proteção de dados pessoais de crianças e adolescentes: um debate sobre melhor interesse, (des)equilíbrios, e LGPD a partir do episódio "*arkangel*" da série "*black mirror*". **Revista da Ouvidoria**, Tribunal de Justiça do Estado do Paraná, 2ª edição, 2020, p. 27-51.

SCHWABE, Jürgen. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão**. Uruguai: Konrad Adenauer-Stiftung, 2005.

SILVA, Virgílio Afonso. O proporcional e o razoável. **Revista dos Tribunais***,* v. 798, p. 23-50, 2002.

SOLOVE, Daniel J. **Nothing to hide**: The false tradeoff between privacy and security. Yale University Press, 2011.

SOUZA, Eduardo Nunes. SILVA, Rodrigo da Guia. Tutela da pessoa humana na lei geral de proteção de dados pessoais: entre a atribuição de direitos e a enunciação de remédios. **Pensar Revista de Ciências Jurídicas**, Fortaleza, vol. 4, n. 3, p. 1-22, jul./set. 2019.

STF. Ação Direta de Inconstitucionalidade (ADI) com pedido cautelar proposta pelo Conselho Federal da Ordem dos Advogados do Brasil (CFOAB), perante o Supremo Tribunal Federal (STF), em face da integralidade dos dispositivos estabelecidos pela Medida Provisória nº 954, de 17 de abril de 2020. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=752502168&prcID=5895165#>. Acesso em: 28.11.2020.

STF. **ADI n. 6387**. Relª. Minª. Rosa Weber. Tribunal pleno. Dje: 11.11.2020.

STF. **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade nº 6.387. Relatora**: Minª. Rosa Weber.

STF. **SL 1103**. Rel.: Minª. CÁRMEN LÚCIA. DJE: 05.05.2017.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilística.com**, Rio de Janeiro, ano 9, n. 1, 2020, p. 1-38.

TEPEDINO Gustavo. Premissas metodológicas para a constitucionalização do direito civil. **Revista de Direito do Estado**, Bahia, ano 1, nº 2, abr./jun. 2006, p. 37-53.

TEPEDINO, Gustavo. Crise das Fontes Normativas e Técnica Legislativa na Parte Geral do Código Civil de 2002. In: **A Parte Geral do Novo Código Civil**. 3. ed. Rio de Janeiro: Renovar, 2007.

The Privacy, Data Protection and Cybersecurity Law Review. Alan Charles Raul (Editor). 3. ed. Reino Unido: Law Business Research Ltd, 2016.

ZAGREBELSKY. **El Derecho Dúctil. Ley, Derecho, Justicia**. 8. ed. Madrid (Espanha): Editorial Trotta, 2008.

ZUBOFF, Shoshana, Big Other: Surveillance Capitalism and the Prospects of an Information Civilization, **Journal of Information Technology,** v. 30, p. 75–89. April 4, 2015.

"Coisificação" dos dados pessoais no âmbito das relações contratuais

Patrícia P. Carneiro[140]

RESUMO

A evolução tecnológica tem potenciado um novo mercado, movido por dados pessoais. Os grandes operadores económicos, tendencialmente fornecedores de serviços e conteúdos digitais, fazem da monetização de dados pessoais uma fonte de receita. São várias as injustiças promovidas por este mercado desregulado em que o indivíduo se vê privado de controlo efetivo sobre os seus dados pessoais, e de um modelo de participação equivalente no mesmo. A razão de ser da autonomização dos bens da personalidade e a sua proteção através dos mecanismos dos direitos de personalidade é o ponto de partida para compreendermos as preocupações decorrentes desta nova realidade, e a necessidade de regulação do quadro negocial emergente. Refletimos sobre a conceptualização dos dados pessoais enquanto bens da personalidade ser ultrapassada pela sua "coisificação", reflexo de um cenário prático, reconhecidamente atual, que vê o alcance das suas problemáticas limitado pela defesa de um direito de personalidade.

PALAVRAS-CHAVE

Proteção de dados pessoais; direitos de personalidade; direito de propriedade; coisificação dos dados

[140] Mestre em Direito e Consultora na TekPrivacy Lda.

Commodification of personal data: challenging data protection as a personality right within the Portuguese legal framework

ABSTRACT

Technological evolution has been boosting the creation of a new type of market driven by personal data. Economic operators, who tendentiously are large service and digital content providers, monetize personal data for revenue generation purposes. The absence of a regulated market marks the existence of several "pain points" concerning data subjects' ability to control their personal data and to equally and fairly participate in said market. The reasoning behind arguing that personal data can exist independently of an individual's personality and therefore be subject to a different legal regime from personality rights can be the starting point to understand this new reality concerns and the consequent need to legally regulate this emergent commercial framework. Ultimately, we hereby propose, within the Portuguese legal framework, to accept and conceive personal data as a commodity instead of an aspect of one's personality to overcome the limitations from serving the individuals protection only by evoking a right to personality.

Keywords: personal data protection; personality rights; property rights; commodification of personal data

Introdução

Nos últimos anos temos vindo a observar a monetização de dados pessoais pelas empresas – especialmente, dados do utilizador de serviços e produtos digitais –, fazendo disso a sua principal fonte de receita, causando a emergência e evolução de uma economia digital assim movida e impulsionando toda uma forma de operar no comércio que progrediu com tal celeridade que nos levou a questionar se o Direito conseguiu acompanhar, e se o fez, em tempo útil. Mas, mais que "cortesias comerciais" (pequenas benevolências atribuídas pelas empresas que permitem aos titulares de dados pessoais exercer algum controlo relativamente aos mesmos), as empresas devem fazer corresponder os seus processos de negócio, serviços e produtos, com o disposto no Regulamento Geral sobre a Proteção de Dados ("RGPD" – Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados).

Estes novos modelos de comércio, têm-se mostrado potencialmente negativos para a privacidade da pessoa, que parece não ter ao seu alcance os meios necessários para compreender a repercussão dos seus atos na Internet das Coisas. As pessoas estão privadas de ferramentas que lhes permitam controlo efetivo sobre os seus dados pessoais, e o grau de transparência dos termos de serviço e políticas de privacidade e de tratamento de dados pessoais dos grandes operadores económicos são insuficientes[141].

A esta necessidade de privacidade, somou-se-lhe o âmbito aumentado da dimensão de um poder *de facto* de disposição sobre dados pessoais, assim se conhecendo o surgimento de um direito à proteção de dados pessoais, que obedece a uma regra de "autodeterminação"[142] da pessoa em relação aos seus próprios dados (o indivíduo tem em

[141] Considerando não só a "iliteracia digital", mas também o engodo perpetrado por muitas empresas, como aquele a que hoje vemos nomeado de "*dark patterns*", e que se tem traduzido na aplicação de artifícios, p.e. recorrendo a desenhos enganosos e a linguagem dúbia ou até errónea, que conduzem o indivíduo a uma ação desinformada em benefício próprio da empresa, por exemplo, para que o utilizador de uma página na Internet consinta na recolha dos seus dados pessoais para efeitos da sua comercialização. A este respeito é interessante ver, também a título exemplificativo, uma reflexão sobre o uso de "*dark patterns*" após a entrada em vigor do RGPD no contexto do consentimento para instalação de "*cookies*" no equipamento do utilizador: Midas Nouwens; Ilaria Liccardi; Michael Veale; David Karger; Lalana Kagal – **Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence** [Em linha]. (2020) [Consult. 01-06-2021]. Disponível em WWW: < https://arxiv.org/abs/2001.02479>.

[142] WARREN, Samuel D. e BRANDEIS WARREN dizem-nos que o direito anglo-saxão sempre reconheceu a casa de um Homem como o seu Castelo e que cada Homem é o único e inteiro responsável pelas suas ações e omissões, devendo, com tal, definir quais os exatos aspetos da sua vida que integram o foro da reserva da sua intimidade, sem prejuízo de eventuais interesses superiores (nomeadamente, públicos) prevalecentes. Samuel D.; BRANDEIS, Louis D. – **The right to privacy** [Em linha]. Harvard Law Review. Vol. 4:5, (1890) pp. 193-22 [Consult. 25-05.2019], p. 220. Disponível em WWW:

saber quem armazena os seus dados, porquê, por que meios e durante quanto tempo, e tem a liberdade de deles dispor, controlando-os), e, importa notar, a gradual "coisificação" dos mesmos.

Portanto, deparando-nos com a redação do artigo 3.º, n.º 1, da Lei n.º 12/2005, de 26 de janeiro ("*Informação Genética Pessoal e Informação de Saúde*"): "*A informação de saúde, (...), é* ***propriedade*** *da pessoa (...)"* – negrito nosso, consideramos que mais que saber qual a natureza dos dados pessoais, o cerne da questão pode contribuir para a busca do meio adequado a devolver ao individuo algo que é tão seu – o controlo efetivo sobre os seus dados pessoais.

Este artigo tem como objetivo introduzir um debate sobre a questão de saber a natureza dos dados pessoais e da sua eventual subsunção ao regime da propriedade privada no enquadramento jurídico português. Esperamos que o percurso encetado instigue o discurso dos juristas portugueses, curiosos, e, até, inquietados pela eventual deturpação da identidade e da dignidade de um indivíduo cada vez mais digital.

1. A problemática da "coisificação" dos dados pessoais no âmbito das relações contratuais. Contribuição da Internet das Coisas[143]

Ir ao supermercado já não é o que era.

Se há 5 anos a nossa principal preocupação, enquanto percorríamos os corredores da secção de produtos de limpeza, era saber se haveríamos esquecido de apontar na lista das compras aquele produto que usamos até à exaustão, hoje, existem robôs que o fazem por nós.

É o exemplo da "*ocado.com*", um supermercado em linha[144] que opera no mercado inglês. Segundo Paul Clarke – "*Chief Technology Officer*" na Ocado Retail Limited –, os robôs que "trabalham" nos armazéns automatizados da empresa são capazes de executar o pedido de um cliente com uma média de 50 produtos, em minutos[145]. Esta plataforma de vendas, tem como objetivo permitir ao consumidor fazer as suas compras do mês sem

<http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C>.

[143] Veja-se, a este respeito, o que diz o Centro Nacional de Cibersegurança na sua página na Internet: <https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/>. [Consult. 01-06-2021].

[144] Página na Internet: <www.ocado.com>. [Consult. 01-06-2021].

[145] Do original: "*These robots are capable of collaborating to pick a typical 50-item order in a matter of minutes*". V. CLARKE, Paul – **Ocado is transforming online grocery shopping with AI, but a skills challenge lies ahead**. Harvard Business Review [Em linha]. [Consult. 14-01-2019]. Disponível em WWW: <https://hbr.org/sponsored/2018/05/ocado-is-transforming-online-grocery-shopping-with-ai-but-a-skills-challenge-lies-ahead>.

ter de se deslocar a uma loja física e, até, sem se preocupar com o que apontar na sua lista de compras. A tecnologia utilizada para o efeito, construída com recurso à Inteligência Artificial[146] e ao "*machine learning*"[147], permite prever as necessidades de consumo do cliente e satisfazê-las de forma automatizada, num curto espaço de tempo.

No entanto, é o mercado camuflado que opera em plano de fundo que nos preocupa. A capacidade média atual da tecnologia viabiliza a implementação de processos rápidos de recolha, análise, armazenamento e comunicação de "grandes volumes de dados"[148], usados no mercado por estas empresas como fonte autónoma de lucro. Falar-se-á a este respeito, em "*big data economy*" [149].

Para o exposto, serve igualmente de exemplo a Facebook, Inc. Esta empresa americana é conhecida pela sua plataforma em linha, a rede social Facebook[150], que visa, entre outros aspetos, possibilitar aos seus utilizadores a criação de uma comunidade digital através da qual conseguem, em tempo real, interrelacionarem-se[151]. Tudo isto sem que aos mesmos utilizadores seja exigido o pagamento de algum valor em moeda corrente, a título de contraprestação[152]. Contudo, esta "gratuitidade" tornou-se questionável. Inclusive, a Facebook, Inc. disponibilizava na página inicial da

---

[146] De acordo com o glossário do Conselho da Europa, "*Artificial Intelligence*" (A.I.) é um conjunto de ciências teóricas e técnicas cujo propósito é a reprodução, por uma máquina, das capacidades cognitivas de um ser humano – tradução nossa da definição disponível na página na Internet do Portal Conselho da Europa: <https://www.coe.int/en/web/artificial-intelligence/glossary>. [Consult. 01-06-2021].

[147] Partindo da conceptualização de Inteligência Artificial, "*machine learning*" ou, à letra, aprendizagem das máquinas, é um método de processamento e análise de dados com vista à identificação de padrões e à tomada de decisões automatizadas, em que a intervenção humana é mínima e tendencialmente inexistente. Definição adaptada ao português do texto original disponível numa outra página na Internet da empresa SAS Institute Inc.: <https://www.sas.com/en_us/insights/analytics/machine-learning.html>. [Consult. 01-06-2021].

[148] Este conjunto de atividades de tratamento dados – desde a recolha à sua análise para uso e arquivo –, pode ser identificado como uma cadeia de valor sobre os mesmos (ou "*data value chain*"), um modelo estratégico de negócio voltado para a criação de produtos valorados no mercado, por exemplo, servindo de suporte na tomada de decisões publicitárias de uma empresa através da identificação de segmentos de interesse de clientes, como perfis de consumidores dos seus produtos, desenvolvidos a partir da análise exploratória dos seus dados. V. CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang – **New horizons for a data-driven economy: a roadmap for usage and exploitation of Big Data in Europe** [Em linha]. Springer Open, 2016. [Consult. 14-01-2019]. pp. 17 e 29*ss*. Disponível em WWW: <https://link.springer.com/content/pdf/10.1007%2F978-3-319-21569-3.pdf>. ISBN 9783319215693.

[149] Uma economia movida pelo produto do progresso tecnológico que oferece, pela sua capacidade exploratória e analítica de diversas tipologias de dados em larga escala, novas formas de extrair valor da informação que resulta do seu processamento célere, com vista a tantas finalidades quantas sejam possíveis conceber (otimização de processos, tomada de decisões automatizadas, análises comportamentais, etc.). Sobre o conceito "*Big Data & Analytics*" v. CAVANILLAS, José María; CURRY, Edward; WAHLSTER, Wolfgang – cit. 8, p. 31*ss*.

[150] De domínio: "facebook.com".

[151] Veja-se os Termos de Serviço disponibilizados na página na Internet da Plataforma Facebook: <https://www.facebook.com/terms.php>. [Consult. 01-06-2021].

[152] Página na Internet: https://www.facebook.com/help/186556401394793?helpref=uf_permalink. [Consult. 01-06-2021]).

plataforma[153] bem como no seu centro de apoio ao utilizador, a indicação de que o Facebook é gratuito e de que nunca será pago. "*O Facebook é um site gratuito e nunca vamos exigir que pagues para continuar a utilizá-lo*.", era o que constava na página do centro de apoio ao utilizador em maio de 2019.

Se observarmos o relatório anual de contas da Facebook, Inc. relativo ao ano fiscal de 2017, vemos que a sua principal fonte de receita foi gerada pela publicidade direcionada aos seus utilizadores por terceiros à sua plataforma[154]:

— É registado um crescimento brutal de receitas para a atividade fiscal compreendida entre os anos de 2013-2017 associado a um aumento médio anual de receitas de 47%: de 7,87 para 40,65 mil milhões de dólares americanos, em que 39,94 mil milhões dessas receitas advêm da publicidade direcionada contratada por terceiros[155];

— É registado um aumento de utilizadores ativos: com uma subida anual associada de 14%, quer numa perspetiva diária, quer mensal[156]; e,

— É documentada a valorização do comportamento dos utilizadores por referência à sua zona geográfica, em que o utilizador europeu proporcionou um aumento de receitas com base na sua interação com a publicidade direcionada de 1,41 para 3,19 milhões de dólares americanos[157].

Ficou patente o aumento da procura de espaço publicitário na plataforma da Facebook, Inc., bem como a autonomização da sua oferta enquanto serviço verdadeiramente lucrativo[158]. Um utilizador registado e ativo gratuitamente nesta

---

[153] V. p.e., Qayyah Moynihan; Alba Asenjo - **Facebook quietly ditched the 'It's free and always will be' slogan from its homepage**, *Business Insider* [Em linha]. 27-08-2019. [Consult. 01-06-2021]. Disponível em WWW: <https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-homepage-2019-8>.

[154] "*Substantially all of our revenue is currently generated from third parties advertising on Facebook (…) For 2017, 2016, and 2015, advertising accounted for 98%, 97% and 95%, respectively, for our revenue*.". O relatório anual de contas encontra-se diretamente na página na Internet: < https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_AR_2017_FINAL.pdf>. [Consult. 01-06-2021]; e, juntamente com os relatórios de contas relativos a anos fiscais precedentes, na página na Internet "*Investor Relations*": <https://investor.fb.com/financials/default.aspx>. [Consult. 01-06-2021].

[155] *Idem*, Parte II, item 6 – "*Selected Financial Data*" e item 7 – "*Management's Discussion and Analysis of Financial Condition and Results of Operations*".

[156] *Idem*, Parte II "*Trends in Our User Metrics*".

[157] *Idem*, Parte II– "*Trends in Our Monetization by User Geography*". Com base no texto original: "*The geography of our users affects our revenue and financial results because we currently monetize users in different geographies at different average rates*". Deste ponto do relatório – cit., p. 36 –, resulta clara a pretensão da Facebook, Inc. em atribuir um valor monetário ao seu utilizador.

[158] "*Trends in the number of the users affect our revenue and financial results by influencing the number of ads we are able to show, the value of our ads to marketers, (…)*" – relatório anual de contas da Facebook, Inc. – cit., p. 35.

plataforma não é, em si, rentável. É o registo e a análise da interação do utilizador com a mesma que viabilizada a atribuição de poder económico àquele operador do mercado. Como consequência, a privacidade do utilizador servirá a proteção do capital da empresa, que faz do seu negócio o tratamento de dados pessoais[159]. Se deste mesmo relatório resulta que a organização considera o impacto do RGPD e da alteração política e legislativa nas suas receitas[160], o que igualmente resulta das alterações que a empresa introduziu na página do seu centro de apoio relativa à questão de saber se o uso da plataforma acarreta algum custo para o utilizador[161], certo é que a sua preocupação com a privacidade do utilizador está voltada para a sustentação e sustentabilidade do seu negócio[162].

2. As "maleitas" do mercado de dados

O que se vimos a respeito das plataformas suprarreferidas, acontece com outros operadores em linha que, apercebendo-se do valor da ciência dos dados, passaram a ver no utilizador-final da Internet uma fonte de rendimentos, operando no mercado como instigadores da economia digital[163] por via de um mercado de dados.

Atualmente, os dados pessoais são, pois, fontes de rendimento, tratados como moeda de troca, como objeto de negócio. Histórica e naturalmente são também fonte de inquietude, relacionada com o controlo e o poder de disposição sobre algo[164], determinados bens, de

[159] Reflexo deste enquadramento, é o exemplo ilustrativo plasmado no noticiário eletrónico "SAPO TEK" onde se pode ler em manchete "*Facebook: milhares de credenciais de login estão à venda na Dark Web por 2 dólares*". Artigo disponível em WWW: <https://tek.sapo.pt/noticias/internet/artigos/facebook-milhares-de-credenciais-de-login-estao-a-venda-na-dark-web-por-2-dolares>. [Consult. 01-06-2021].

[160] V. p. 9 do relatório anual de contas da Facebook, Inc. – cit.

[161] Onde agora podemos ler, em alternativa ao acima mencionado: "*Nota: o Facebook não vende as tuas informações e não partilhamos informações que te identifiquem pessoalmente (informações como o teu nome ou endereço de e-mail que, por si só, podem ser utilizadas para te contactar ou identificar), a menos que nos dês permissão.*".

[162] Para o original, cf. Relatório anual de contas da Facebook, Inc. – cit., p. 13.

[163] Remetemos para LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Trading data in the digital economy: legal concepts and tools**. Münster Colloquia on EU Law and the Digital Economy III. Alemanha: Nomos Verlagsgesellschaft, 2017, p. 13. Segundo os Autores, quando se fala em economia digital deve haver o cuidado de compreender que, em última linha, estamos a falar do formato de economia de mercado global, que se tornará digital.

[164] Trazemos à colação a distinção entre "dados pessoais", "dados públicos" e "dados confidenciais" introduzida pela já revogada Lei n.º 10/91 da "*Protecção de Dados Pessoais face à Informática*". Cremos que poderá evidenciar flagrantemente a vontade de apropriação pública da "pessoalidade" de determinados dados pessoais, por oposição à legislação atualmente aplicável e cujo objetivo, sem prejuízo de salvaguarda dos interesses públicos, é atribuir às pessoas o controlo sobre os seus dados pessoais. Sobre a distinção entre os conceitos de "dados públicos" e de "dados pessoais", MARQUES, José Augusto Garcia; SILVEIRA, Luís Lingnau da – Pareceres: **vida privada – utilização da informática**. Lisboa: Procuradoria-Geral da República, 1998, pp. 476ss, Parecer N.º 23/95. Neste assunto também, PINHEIRO, Alexandre Sousa: "*Trata-se (...) de uma forma perigosa de proceder à proteção de dados de dados pessoais, contaminada pela ideia de que a protecção de dados se integra no domínio da privacidade e que os seus*

caráter de um modo tendencial intrinsecamente humano. Neste sentido, é essencial salvaguardar direitos fundamentais invioláveis, visualizar cenários de risco que, em casos extremos, implicarão situações como a de fraude, usurpação de identidades e tráfico de pessoas. Não obstante, as novas gerações provaram ser criadas de matéria digital e, parte da consequência de permitir à pessoa o controlo e a disposição sobre os seus próprios dados, está em ser ela mesma a definir onde começa e onde acaba o seu espaço mais privado – a sua informação pessoal –, para o qual deseja proteção. Devemos, por tudo isto, permitir a influência do avanço tecnológico na recriação das nossas necessidades.

Os contornos de um problema começaram a desenhar-se por referência à emergência de um mercado não especificamente regulado dotado das condições necessárias à criação de monopólios de dados. Por um lado, está instalado o meio que facilita a partilha de dados pessoais do utilizador da Internet das Coisas; por outro, estes mesmos dados são extraídos de forma abusiva pelos intervenientes de maior poder económico, que atuam em função de interesses financeiros próprios, através da comercialização de dados pessoais. Sendo indubitável que os dados pessoais sustentam vários aspetos da economia digital, vários são os indícios da nefasta influência desta economia na dignidade da pessoa ao nível dos seus direitos fundamentais, como o seu direito à privacidade e à proteção de dados pessoais[165]. Os instrumentos que compõem o dia-a-dia do cidadão desta nova era que vive na "*cloud*" são verdadeiras armadilhas de recolha de dados pessoais, tornando-se cada vez menos propício conceber um mundo no

elementos mais afastados da reserva privada merecem uma tutela diminuída por parte do Direito" (v. PINHEIRO, Alexandre Sousa – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional**. AAFDL, 2015, pp. 701ss. ISBN 9786120002605).

[165] Este pode ser o enquadramento até de uma possível crise ética, moral e legislativa. Neste sentido, dos riscos éticos e morais do grande processamento de dados pessoais sobre os direitos fundamentais das pessoas, as orientações "*guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*" do Comité Consultivo da Convenção para a Proteção das Pessoas face ao tratamento automatizado dos dados de caráter pessoal (em WWW: <https://rm.coe.int/t-pd-2017-1-bigdataguidelines-en/16806f06d0>. [Consult. 01-06-2021]). Repare-se no seguinte exemplo: em março de 2018, o jornal "*The Guardian*" publicava notícia a expor a violação de dados pessoais promovida pela empresa Cambridge Analytica Ltd. Esta empresa tinha utilizado a rede social Facebook para recolher dados pessoais sobre os seus utilizadores de forma a definir os seus perfis e a utilizá-los no mercado, sem o seu conhecimento ou autorização. Em maio de 2018, o mesmo jornal falava na venda de dados na "*dark web* (v. PRESS ASSOCIATION – **Hacker jailed for selling Asda and Uber customers' data on dark web**, *The Guardian* [Em linha]. 25-05-2018. Disponível em WWW: <https://theguardian.com/technology/2018/may/25/hacker-jailed-for-selling-asda-and-uber-customers-data-on-dark-web>).

qual possamos ser anónimos e onde não sejamos assombrados pela nossa própria "pegada digital"[166]. É ilustrativo, o caso dos "*smart glasses*" da Google, Inc.[167].

A Google desenvolveu um par de óculos que funciona como um pequeno computador com ligação à Internet e um conjunto de funcionalidades adicionais associadas, entre as quais, a de tirar fotografias, de filmar e a de transferir os dados captados – em tempo real – para o telemóvel do seu utilizador. A sua comercialização foi contestada por motivos relacionados com a privacidade e a proteção dos dados pessoais não só do utilizador do equipamento, mas, também, de eventuais indivíduos com quem este se cruzasse usando aqueles mesmos óculos. A Autoridade Europeia para a Proteção de Dados Pessoais ("AEPDP"), no seu "*Technology Report No 1*"[168], vem-nos explicar o porquê de esta tecnologia não ser "*privacy-friendly designed*". Em jeito de súmula: o equipamento tanto admite a hipótese de o seu utilizador tratar dados pessoais de não-utilizadores de forma camuflada, designadamente, recolhendo registos de imagens e/ou de voz dos mesmos sem que estes se apercebam; como as próprias configurações incluem a captação de dados de não-utilizadores dos óculos que estejam nas proximidades do seu utilizador, como por exemplo, a sua localização. Ademais, a apropriação desta informação por terceiros através de ciberataques demonstrou-se altamente viável, pela fragilidade do seu sistema.

Neste seguimento, é pertinente saber se este mercado é legalmente admissível, se será viável do ponto de vista da tutela dos direitos fundamentais e em que medida pode servir a pessoa, protegendo a dignidade humana.

---

[166] Por menor que seja a intensidade da atividade do utilizador na Internet, estará a contribuir para a construção de um retrato incremental sobre a sua pessoa, tornando-se mais realista à medida em que essa atividade de utilização da Internet aumenta. Este retrato do utilizador é a sua "*digital footprint*". V. o esquema de sensibilização para o assunto da organização Internet Society na sua página na Internet: <https://www.internetsociety.org/tutorials/your-digital-footprint-matters/>. [Consult. 01-06-2021]. Pinheiro, Alexandre Sousa – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional** – cit., p. 225, preferiu o termo "tatuagem digital".

[167] EUROPEAN DATA PROTECTION SUPERVISOR – **Smart glasses and data protection, Technology Report No 1** [Em linha]. (2019) [Consult. 25-05-2019]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/19-01-18_edps-tech-report-1-smart_glasses_en.pdf>.

[168] EUROPEAN DATA PROTECTION SUPERVISOR – **Smart glasses and data protection, Technology Report No 1** – cit.

3. O Mercado Único Digital

3.1. Enquadramento de uma estratégia

O "*boom*" do desenvolvimento tecnológico que temos vindo a abordar, tem sido designado como "revolução 4.0" (ou 4.ª revolução industrial). Desde este fenómeno que verificamos uma Europa cada vez mais ciente da necessidade de assumir as rédeas de um novo mercado económico em expansão, o mercado económico digital. Em 2013, a Comissão Europeia estudava já como fazer com que os dados pessoais "*funcionassem da melhor forma para a economia digital europeia*". Em maio de 2015, nasce o Mercado Único Digital – ou "*Digital Single Market*" ("DSM") –, marcado pela consciência de que "*a internet e as tecnologias digitais estão a transformar a nossa vida (…) à medida que se integram mais profundamente em todos os setores da nossa economia e da nossa sociedade*[169]", a par de renovadas preocupações relacionadas com a proteção de dados pessoais que o legislador sabe não poder descurar e, concretamente, o RGPD.

3.2. A Diretiva (EU) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019 sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais

Do DSM decorreu igualmente a Diretiva (EU) 2019/770 do Parlamento Europeu e do Conselho de 20 de maio de 2019 sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais (doravante, apenas "Diretiva (EU) 2019/770")), que introduziu uma novidade no quadro dos contratos de consumo, concretamente, de conteúdos e serviços digitais.

No âmbito da exploração da licitude de um mercado de dados (pessoais), parece-nos relevante apontar para algumas particularidades subjacentes ao processo legislativo relativo à Diretiva (EU) 2019/770, e, em particular, para o texto da respetiva Proposta de Diretiva do Parlamento Europeu e do Conselho, de 2015[170] (doravante, apenas "Proposta"), que revela a pretensão de o legislador regular o contrato a título oneroso que tem como contrapartida o fornecimento ativo de dados (incluindo dados pessoais), sem

[169] COM(2015) 192 final, pp. 420 e 423– onde também se reconhece que "*daqui a menos de uma década, a maior parte da atividade económica dependerá de ecossistemas digitais que integrem infraestruturas digitais, hardware e software, aplicações e dados*.".
[170] COM(2015) 634 final.

prejuízo da *"proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais*"[171].

Esta solução trouxe consigo a perceção de que o legislador europeu, não descurando da posição do consumidor enquanto titular de dados pessoais ao abrigo do RGPD, reconhece que "*na economia digital, as informações sobre os indivíduos são muitas e cada vez mais vezes consideradas pelos participantes no mercado como tendo valor comparável ao do dinheiro*[172]". A solução que a Proposta ofereceu, e que a Diretiva (EU) 2019/770 de uma forma geral acolheu, considerou o valor transacional dos dados pessoais fornecidos e procurou estabelecer o equilíbrio negocial entre as partes no âmbito de um esquema contratual até então negligenciado, e que tem promovido "*incentivos injustificados*" para os fornecedores de conteúdos e serviços digitais.

Foram várias as vozes que se exaltaram com receio de que o legislador não estivesse a ser suficientemente cuidadoso em matéria de privacidade e de proteção de dados pessoais[173]. Todavia, não nos parece plausível retirar do texto da Proposta o

[171] Veja-se o art.º 3.º da Proposta relativo ao seu âmbito de aplicação.

[172] Cf. Considerando (13) da Proposta: "*Os conteúdos digitais são frequentemente fornecidos (…) pela concessão de acesso a dados pessoais (…) Introduzir uma diferenciação dependendo da natureza da contrapartida (…) iria fornecer um incentivo injustificado para as empresas passarem a oferecer conteúdos digitais em troca de dados. (…) os defeitos das características de desempenho dos conteúdos digitais fornecidos, face a contrapartidas que não dinheiro, poderão ter um impacto nos interesses económicos dos consumidores (…)*.".

[173] Foi o caso da "EDPS" (European Data Protection Supervisor) ou AEPDP no seu parecer relativo à Proposta (**Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content** [Em linha]. (14-03-2017) [Consult. 25-05-2019]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf>); e respetivo sumário (**Summary of the Opinion on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content** [Em linha]. 2017/C 200/07. (23-06-2017) [Consult. 25-05-2019]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/17-06-23_opinion_digital_content_ex_summ_en.pdf>). Reconhecendo a importância da "*economia dos dados para o crescimento da UE*", a Autoridade Europeia para a Proteção de Dados Pessoais reivindicou que os dados pessoais nunca poderão ser considerados meras mercadorias, por tal ser incompatível axiologicamente com o núcleo de proteção dos direitos fundamentais em causa (i.e., a dignidade da pessoa), como o direito à proteção de dados pessoais. Ora, concordamos que é preciso averiguar a justa medida em que os bens jurídicos "dados pessoais" possam ser objeto de contraprestação, e que o texto da Proposta ficou aquém do expectável, especialmente, no campo dos conceitos e definições. Posto isto, se a EDPS prevê como problemático entendermos os dados pessoais como contraprestação pela incapacidade de os indivíduos avaliarem economicamente os mesmos, ou de a sua cedência não poder privar o consumidor de os facultar novamente a outro operador, parece-nos pertinente indagar sobre a aplicabilidade de um regime jurídico capaz de regular estas trocas em sede jus-civilística e que não passe necessariamente pela tutela dos direitos de personalidade, como por exemplo, o regime jurídico da propriedade privada. O que não significaria uma desconsideração da proteção que o RGPD pretende conferir, pelo contrário, o regime jurídico aplicável teria de ser complementar. Por fim, e como de seguida expomos, também não concebemos razão para a EDPS simultaneamente se afastar do conceito de contraprestação e rejeitar o termo "remuneração", atentando no seu argumento de que tal abordagem não tem em conta a "*natureza de direitos fundamentais da proteção de dados pessoais*" (veja-se o seu parecer sobre a proposta legislativa "um novo acordo para os consumidores" – **EDPS Opinion 8/2018 on the legislative package "a new deal for consumers"** [Em linha] (5-10-2018) [Consult. 25-05-2019]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/18-10-05_opinion_consumer_law_en.pdf>) e o

desvirtuamento do núcleo essencial destes direitos. Ao invés, tal solução, potencia o controlo dos dados pessoais pelo seu titular, permitindo-lhe participar na estratégia de economia que é o mercado de dados pessoais, com os aqueles (dados pessoais) que gera. Nomeadamente, pela não "discriminação" de modelos de negócio considerados gratuitos pelo facto único de serem fornecidos dados pessoais pelo seu titular por oposição ao pagamento de um preço. Atentando na globalidade do texto da Proposta, entendemos que estava em conformidade com o atual quadro legal europeu de proteção das pessoas naturais no que se refere ao tratamento dos seus dados pessoais, concretamente, com o RGPD, com a Diretiva relativa à privacidade e às comunicações eletrónicas ainda em vigor[174], e com a proposta de Regulamento que visa revogar esta Diretiva. Este cuidado na harmonização do segmento legislativo em construção é, aliás, o que resultou claro da exposição de motivos da Proposta: "*A aplicação e execução da presente proposta devem ser efetuadas em total conformidade com esse quadro jurídico*".

Vejamos alguns pontos específicos do seu texto.

De acordo como o art.º 13.º da Proposta, sob a epígrafe "*rescisão*", se o consumidor rescindisse um contrato no âmbito do qual, em alternativa ao pagamento de um preço, tivesse fornecido dados pessoais, o fornecedor dos conteúdos ou serviços digitais passaria a dever abster-se de utilizá-los. Esta situação, não foi, porém, acatada no texto final da Diretiva (UE) 2019/770[175]. No entanto, uma vez que o circunstancialismo da rescisão, pelo consumidor, nos termos da Proposta, seria o da verificação da existência de um fornecimento desconforme que afete as características principais do objeto contratual, tal solução seria conciliável com os direitos dos titulares dos dados pessoais consagrados no RGPD, designadamente e a título exemplificativo, com o direito de o titular retirar o consentimento a qualquer momento regulado no n.º 3 do art.º 7.º do

respetivo sumário – **Summary of the Opinion of the European Data Protection Supervisor on the legislative package "a new deal for consumers"** [Em linha]. 2018/C 432/04. (30-11-2018) [Consult. 25-05-2019]. Disponível em WWW: <https://edps.europa.eu/sites/edp/files/publication/19-01-04_opinion_new_deal_consumers_summary_en.pdf>.

[174] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

[175] Que remete, sempre que possível, para o RGPD, quando alguma especificidade do contrato tenha que ver com o facto de o consumidor ter fornecido/prometido fornecer dados pessoais em troca do fornecimento serviço ou do conteúdo digital – cf. Os seus Considerandos (37), (38), (39), (48) e (69), e o art.º 16.º, n.º 2.

RGPD[176], cujos efeitos práticos seriam equivalentes aos de uma rescisão contratual[177]. Ainda assim, não nos parece plausível um direito de rescisão ilimitado no seu escopo e incondicional na sua invocação; antes, questionamos a dimensão da medida em que a "discriminação" entre os modelos de negócio suprarreferidos e que fundamenta a sua regulação, é plausível. Pensamos nas situações em que o consumidor reclame a proteção dos dados pessoais que alienou em troca dos serviços e/ou dos conteúdos solicitados. Se o consumidor trata os seus dados pessoais de acordo com a sua valorização no mercado, fazendo um uso utilitário dos mesmos, deverá poder reivindicar a sua proteção irrestritamente?

Perante tal cenário, cremos que o operador económico sairia injustamente financeiramente prejudicado se o titular pudesse reivindicar a proteção dos seus dados pessoais ilimitadamente, tal como sairia se o consumidor exigisse a devolução do preço pago, sem mais. O que não se pode considerar razoável num mercado onde, entendemos, é de destacar a autonomia da vontade do titular dos dados pessoais. A este respeito, e em consonância com o n.º 3 do artigo 7.º do RGPD (onde se lê: "*A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado*"), cumpre-nos apontar para dois dos institutos de direito civil que se pautam pela valorização ética do plano jurídico. Reportamo-nos ao princípio geral da boa-fé, e, em particular, a um dever lateral[178] de boa-fé, que sempre limitará a liberdade de atuação das partes e, neste caso, dos titulares que "mudaram de ideia" quanto à comercialização dos seus dados pessoais, sem respeito pela perfeição do negócio jurídico (cf., p.e., art. 762.º, n.º 2 do Código Civil Português – "C.C."); e, até em tom complementar ao que abaixo refletimos neste texto a respeito da funcionalização de direitos subjetivos, concretamente, do direito à proteção de dados pessoais e do direito de propriedade privada, ao princípio do abuso do direito (art. 334.º do C.C.), no âmbito da

[176] Sendo que o tratamento lícito de dados pessoais (não sensíveis) vem regulado no art.º 6.º do RGPD e que, entre outros fundamentos legais, impõe que o titular dos dados tenha consentido para uma ou mais finalidades específicas do seu tratamento. Não queremos, com isto, assumir que a base de licitude do tratamento de dados pessoais facultados em troca, por exemplo, de um serviço digital, será sempre e necessariamente o consentimento do titular dos dados pessoais; mas, neste caso, o ónus da prova de um consentimento válido porque em conformidade com o RGPD, especialmente no que concerne ao seu caráter livre (o que se poderia questionar, ilustrativamente, no caso de não ser dada ao titular a possibilidade de escolher entre ceder os seus dados em troca de um serviço, ou pagar o respetivo preço), sempre seria do operador económico. Ademais, em conformidade com o n.º 4 do art.º 7.º do RGPD.

[177] Remetemos para Fryderyk Zoll em SCHULZE, Reiner; STAUDENNMAYER, Dirk; LOHSSE, Sebastian – **Contracts for the supply of digital content: regulatory challenges and gaps**. Münster Colloquia on EU Law and the Digital Economy II. Alemanha: Nomos Verlagsgesellschaft, 2017, pp. 182*ss*.

[178] COSTA, Mário Júlio de Almeida – Direito das obrigações. 12ª ed. rev. e at. (Manuais Universitários), pp. 77*ss*. ISBN 978-972-40-4033-2.

modalidade "*venire contra factum proprium"*. Ora, esta retirada do consentimento para o tratamento de dados pessoais pelo consumidor, titular desses mesmos dados, poderá lesar injustificada e desproporcionalmente os interesses do operador económico, que sempre teria o direito a ser indemnizado pelos danos dessa cessação antecipada injustificada e imprevista. Em última linha, consideramos que, ao operador económico lesado, poderá atribuir-se legitimidade para continuar a tratar os dados que lhe haviam sido fornecidose enquanto o consumidor não o ressarcir pelas suas perdas, na medida em que tal atuação não traduza um sacrifício desproporcional dos direitos do titular[179]. Sem prejuízo, notamos, de o legislador dever acautelar as garantias adequadas, por exemplo, tal como havia definido na Proposta a respeito das relações contratuais de tempo indeterminado ou de longa duração (cujo período de execução se prolongasse por mais de 12 meses), em que o consumidor podia rescindir o contrato findos os primeiros 12 meses[180]. Neste seguimento, embora o texto da Diretiva (UE) 2019/770 aponte para soluções distintas das que a Proposta salvaguardou e que viemos referindo, não obsta ao entendimento de que o consumidor que aliene dados pessoais em troca do fornecimento de serviços e/ou conteúdos digitais, findo o período acordado entre as partes ou perante a verificação da prestação de um serviço não conforme, possa rescindir tal contrato[181]. Sempre sob pena de potenciarmos a falência do mercado digital.

Para efeitos de proteção dos dados pessoais, o quadro contratual previsto na Proposta, estaria, assim, longe de significar que a valorização económica de dados pessoais se traduz numa desvantagem para o seu titular. Pelo contrário, motiva-nos o raciocínio de que é este o tipo de incentivo legislativo que permite assegurar o direito fundamental à proteção de dados pessoais num mercado atípico, aliado à possibilidade de o titular dos dados pessoais - e consumidor- livremente (e conscientemente) deles dispor. Ademais, podemos continuar a atentar no mesmo art.º 13.º da Proposta que, diferentemente da Diretiva (UE) 2019/770, previu que o fornecedor, em caso de rescisão

[179] A respeito da lesão dos interesses económicos do operador que aceite dados pessoais como "forma de pagamento" ou que os "compre", Christiane Wendehorst argumentou que os riscos inerentes ao investimento, como o caso de o titular dos dados pessoais retirar o consentimento, são atenuados pelos "*Notice and Choice Principles*", segundo os quais, a entidade que pretende transferir os dados pessoais em apreço deverá, previamente à transferência, cumprir um conjunto de obrigações de informar o titular e dar-lhe a possibilidade de se opor à mesma. Cf. LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Trading data in the digital economy: legal concepts and tools** – cit., pp. 344-346.

[180] Cf. Considerando (46) e o art.º 16.º da Proposta.

[181] Apesar de no texto do seu art.º 16.º, n.º 2, se limitar a referir que o profissional deve cumprir as obrigações decorrentes do RGPD, no seu considerando (67) prevê que caso "*o consumidor tenha fornecido dados pessoais, deverá (…) também* [ter] *direito a rescindir o contrato*".

e sem que seja necessário um pedido do consumidor neste sentido[182], deve "*fornecer ao consumidor os meios técnicos para recuperar a totalidade dos conteúdos fornecidos pelo consumidor e quaisquer outros dados produzidos ou gerados através da utilização, pelo consumidor, dos conteúdos digitais (…)*"; e, que, o consumidor tem o direito "*a recuperar o conteúdo, a título gratuito, sem grave inconveniente, num prazo razoável e num formato de dados geralmente utilizado.*". Também esta solução estaria, assim o entendemos, de acordo com as exigências do RGPD decorrentes da matéria de exercício de direitos do titular de dados pessoais. Em primeiro lugar, não prejudicaria o direito de acesso aos dados pelo seu titular nos termos do art.º 15.º do RGPD, que abrange a possibilidade de o titular obter informações relativamente às operações de tratamento conduzidas pelos responsáveis pelo tratamento (como o são os fornecedores) sobre os seus dados pessoais, e o direito a obter uma cópia dos dados pessoais em fase de tratamento[183]. Em segundo lugar, estaria alinhada com o bom exercício do direito ao apagamento dos dados regulado no art.º 17.º do RGPD; e, seria compatível com o direito de portabilidade do art.º 20.º do RGPD[184].

Com isto, não desconsideramos as preocupações manifestadas no relatório do Parlamento Europeu e do Conselho que refletiram sobre a Proposta[185], concretamente, quando nas alterações sugeridas surgiu reforçada a ideia de que os dados pessoais não podem ser tratados como meras mercadorias. Partilhamos de alguma apreensão quanto ao impacto negativo na economia do consumidor causado pelo fornecimento, desregulado, de um serviço ou conteúdo digital no qual tenham sido fornecidos dados pessoais em detrimento do pagamento de um preço. Como tal, não nos surpreende que, preferindo a expressão "*em troca de dados pessoais*" por oposição à expressão "*por uma*

[182] Cfr. com o art.º 16.º, n.º 4, da Diretiva (UE) 2019/770.

[183] Aliás, o n.º 3 do art.º 15.º do RGPD prevê que o fornecedor no âmbito da Proposta, responsável pelo tratamento de dados pessoais ao abrigo do RGPD, perante tais pedidos "*pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos*". Esta solução, acaba por se ver afastada quando o titular dos dados pessoais figura como consumidor (e, se, *"o titular dos dados apresentar o pedido por meios eletrónicos, (…) salvo pedido em contrário do titular dos dados,* [caso em que] *a informação é fornecida num formato eletrónico de uso corrente"*).

[184] Neste seguimento, também discordamos do entendimento da EDPS (**Opinion 4/2017** – cit.) quando referiu que existe uma questão de sobreposição de tutela entre os artigos 15.º e 16.º da Proposta e os artigos relevantes do RGPD relativos aos direitos dos titulares dos dados pessoais. A eventual inconsistência que se possa retirar da comparação dos dois normativos resultaria, assim, e, em nosso entender, do seu caráter complementar e não derrogatório.

[185] Relatório sobre a Proposta do Parlamento Europeu, de 27-11-2018 (COM(2015)0634 – C8-0394/2015 –2015/0287(COD) [Em linha]. 2015/0287(COD) [Consult. 07-07-2019]) e na Diretiva então aprovada (Diretiva (UE) 2019/770). Disponível em WWW: <http://europarl.europa.eu/doceo/document/A-8-2017-0375_PT.html?redirect>.

contrapartida que não dinheiro"[186], se continue a reconhecer que os dados pessoais têm valor comparável ao dinheiro. Assim como não nos causa estranheza que, na Proposta, o legislador tenha procurado o enquadramento destas iniciativas legislativas no quadro do Direito do consumidor no comércio eletrónico, em contexto de uma economia digital, justamente por aqueles modelos de negócio específicos[187] se aplicarem *"**já** de diferentes formas numa parte considerável do mercado*[188]" – negrito nosso. Situação legal que, aliás, se manteve com a Diretiva (UE) 2019/770.

As referências mais contestadas e que dessa forma realçamos da Proposta (como a adoção da terminologia "*contrapartida que não dinheiro*" para definir e concretizar o fornecimento de dados pessoais pelo consumidor em troca de conteúdos ou serviços digitais), não foram adotadas na Diretiva (UE) 2019/770. Em todo o caso, entende-se que a Diretiva (EU) 2019/770 mantém a essência de que os dados pessoais são considerados uma contrapartida, ainda que do seu texto isso não resulte expresso[189], e o legislador não se abstém de considerar que devem ser alocadas as ferramentas idóneas à proteção do consumidor, como o direito a meios de ressarcimento ao abrigo do contrato[190] quando este, em troca de conteúdos ou serviços digitais, forneça os seus dados pessoais ou se comprometa a fazê-lo em alternativa ao pagamento de um preço.

Apontamos ainda, aproveitando este seguimento, para o facto de a Comissão Europeia, nas suas subsequentes iniciativas legislativas com o intento não só assegurar uma melhor aplicação das normas da UE em matéria de defesa do consumidor, como garantir a sua modernização[191], ter mantido a sua posição relativamente à monetização dos dados pessoais, não obstante o relatório do Parlamento Europeu sobre a sua

---

[186] COM(2015)0634 – C8-0394/2015 – 2015/0287(COD) – cit. V., por exemplo, a alteração 19 ao Considerando (13) da Proposta.

[187] COM(2015)0634 – C8-0394/2015 – 2015/0287(COD) – cit.: *"Alteração 21(...) (14) (...) a presente diretiva deverá ser aplicável aos contratos em que o operador solicita e o consumidor lhe entrega dados pessoais e aos casos em que o operador recolhe dados pessoais"*. Notamos que nos vamos abster de maiores comentários a esta sugestão de alteração e vamos limitarmo-nos a apontar para a nossa preocupação que se levanta no seguimento do último parágrafo sugerido: "*Também não se deverá aplicar a situações em que o consumidor esteja exposto a anúncios com o intuito exclusivo de aceder a conteúdos digitais ou a um serviço digital"*.

[188] Cf. alteração 20 da COM(2015)0634 – C8-0394/2015 – 2015/0287(COD) – cit.

[189] Neste sentido, Sebastian Lohsse; Reiner Schulze; Dirk Staudenmayer em LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Data as Counter-Performance – Contract Law 2.0?**. Münster Colloquia on EU Law and the Digital Economy V. Alemanha: Nomos Verlagsgesellschaft, 2020, pp. 9*ss*.

[190] V. Considerando (24) da Diretiva (UE) 2019/770.

[191] Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, a Diretiva 98/6/CE do Parlamento Europeu e do Conselho, a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho e a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das normas da UE em matéria de defesa do consumidor (COM/2018/185 final – 2018/0090(COD)).

Proposta[192] e os pareceres da AEPDP suprarreferidos, cujos conteúdos apontam para a impossibilidade de coexistência da "coisificação" dos dados pessoais com a sua proteção, assim evidenciando a coerência normativa refletida *supra*. "*Remuneração*" foi a terminologia utilizada para caracterizar esta valorização na exposição de motivos da Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, a Diretiva 98/6/CE do Parlamento Europeu e do Conselho, a Diretiva 2005/29/CE do Parlamento Europeu e do Conselho e a Diretiva 2011/83/UE do Parlamento Europeu e do Conselho, a fim de assegurar uma melhor aplicação e a modernização das normas da UE em matéria de defesa do consumidor. E, embora esta terminologia não tenha sido adotada no corpo da versão final da Diretiva[193], o seu texto partiu do pressuposto que o crescimento do comércio eletrónico depende da recuperação da confiança do consumidor e, consequente e assumidamente, da valorização económica dos dados pessoais que este fornece como moeda de troca para obter serviços ou conteúdos digitais[194], em detrimento do enquadramento destes serviços/conteúdos como "gratuitos".

No sentido de enquadrar a tutela do utilizador dos serviços digitais ditos "gratuitos" no regime jurídico da proteção do consumidor, escreviam Chris Jay Hoofnagle e Jan Whittington[195]. Para estes Autores, a divulgação e a promoção de serviços digitais como gratuitos quando a oferta dos mesmos implica que o seu fornecedor trate dados pessoais recolhidos ou fornecidos pelo seu titular naquele contexto, mais do que uma ilusão, é verdadeiramente decetivo. Argumentaram que neste tipo de transações não estão a ser ponderados os verdadeiros custos suportados pelos utilizadores destes serviços[196], que veem a sua privacidade anulada em prol do enriquecimento desmesurado do operador económico. Dão-nos o panorama, quase surrealista, do fornecimento da morada pelo utilizador do serviço, em que este, para conseguir resguardar a localidade da

[192] COM(2015)0634 – C8-0394/2015 – 2015/0287(COD) – cit.
[193] Diretiva (UE) 2019/2161 do Parlamento Europeu e do Conselho de 27 de novembro de 2019 que altera a Diretiva 93/13/CEE do Conselho e as Diretivas 98/6/CE, 2005/29/CE e 2011/83/UE do Parlamento Europeu e do Conselho a fim de assegurar uma melhor aplicação e a modernização das regras da União em matéria de defesa dos consumidores.
[194] Sobre a conversão dos dados pessoais num "produto de valor comercial", a sua utilização como "método de pagamento" de serviços gratuitos, e sobre a assimetria informacional, v. p.e., GRUNDMANN, Stefan – **European Contract Law in the Digital Age**. Cambridge: Intersentia, 2018, pp. 27*ss* e 40*ss*.
[195] V. HOOFNAGLE, Chris Jay; WHITTINGTON, Jan **– Free: accounting for the costs of the internet's most popular price**. UCLA Law Review. 61 (2014), pp. 606-670, pp. 557ss.
[196] Neste sentido, LAUDON, Kenneth C. – **Markets and Privacy** – cit., p. 93*ss*. Segundo o autor, o custo da "invasão" da privacidade do individuo é muito inferior ao seu custo social, para o próprio; defendendo que a informação pessoal dos indivíduos está a ser utilizada de forma ineficiente causando desperdícios. Cf. LAUDON, Kenneth C. – cit., p. 99.

sua residência habitual, teria, em última linha, de suportar os custos associados à sua alteração, como a compra de uma nova habitação. Adicionalmente, Hoofnagle e Whittington[197] previram que este regime de tutela do consumidor de serviços digitais poderia ser complementado com a atribuição de direitos de propriedade ("*ownership rights*") ao consumidor sobre a sua informação pessoal. Os consumidores passariam a ter maior capacidade negocial e, consequentemente, não só poderiam controlar a utilização dos seus dados pessoais pelos operadores económicos, como condicionariam o seu fornecimento a maiores garantias de privacidade. Quanto a este último aspeto, cremos que medidas como as "*privacy by design and privacy by default*"[198] são de grande relevância quando se trata de conservar padrões de qualidade de serviço que devem considerar a privacidade e a proteção dos dados pessoais do consumidor, titular de dados pessoais, desde a sua conceção e por defeito.

4. Indagação sobre a aplicabilidade do regime do jurídico da propriedade privada

Continuando no cenário em que observamos práticas correntes, banalizadas, de "troca" de dados pessoais, e um legislador europeu que se preocupou em introduzir ao debate o conceito de contraprestação para caracterizar estes bens – os dados pessoais – como objeto de relações jurídicas, surge a questão de saber sobre a sua natureza: o alcance da tutela da privacidade da pessoa e a necessidade de lhe serem atribuídos meios de controlo eficazes sobre os seus dados pessoais pelo ordenamento jurídico permitirá a coexistência com a sua (tendencial e "*de facto*") "coisificação"?

Na CRP76 o direito à autodeterminação informativa[199] surge como um direito pessoal inominado e, para alguns autores, é uma das expressões do direito ao desenvolvimento da personalidade, na sua vertente de "*direito a auto-afirmação*"[200], tal como plasmado no n.º 1 do artigo 26.º sob a epígrafe "*outros direitos pessoais*". Neste preceito, estão também consagrados os direitos "*à identidade pessoal*", "*ao desenvolvimento da personalidade*", e à "*reserva da intimidade da vida privada e*

[197] HOOFNAGLE, Chris Jay; WHITTINGTON, Jan – **Free: accounting for the costs of the internet's most popular price** – cit., p. 664.
[198] Reveja-se a COM(2015)0634 – C8-0394/2015 – 2015/0287(COD) já referida, onde esta preocupação é patente. Compare-se, por exemplo, a alteração 23 à Proposta e o Considerando introduzido (15-A); a alteração 31 à Proposta e o Considerando introduzido (22-A); a alteração 39 e o Considerando aditado (28-A); a alteração 99 à Proposta e o artigo aditado 6.º-A; e, a alteração 108 à Proposta e o artigo aditado 12.º-A.
[199] Sobre a origem do termo veja-se PINHEIRO, Alexandre Sousa – cit., pp. 429*ss*.
[200] CANOTILHO, J. J. Gomes; MOREIRA, Vital – **CRP Constituição da República Portuguesa anotada**. Vol. I, 4.ª ed. rev. e reimp. Coimbra: Coimbra Editora, 2007, p. 464, parágrafo IV da anotação ao art.º 26.º.

familiar"; e, a garantia constitucional "*contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias*" – é o que resulta dos números 1 e 2 do artigo 26.º da CRP76.

O direito à identidade pessoal vai no sentido de tutelar "*aquilo que identifica cada pessoa como indivíduo*"[201] – como é o caso do nome da pessoa e, consequentemente, da tutela do direito ao nome. Por sua vez, da densificação do direito ao desenvolvimento da pessoa[202] resulta que em causa está o reconhecimento da liberdade de esta se formar enquanto tal, sem a ingerência de forças desproporcionais e desconformes em geral sobre o seu espaço (também) jurídico de atuação. Ou seja, aqui não só se pretende tutelar a disponibilidade da pessoa para "ser" – criando-se enquanto indivíduo, único, diferenciável[203] –, como se pretende proteger a sua autonomia, a sua liberdade em optar pela via da privacidade em relação àquilo que se tornou – a sua zona de reserva da intimidade da sua vida –, ou em se expor na comunidade em que se insere[204] – ainda que se trate de uma comunidade digital. Por fim, quanto ao direito à reserva da intimidade da vida privada, J. J. Gomes Canotilho e Vital Moreira, reconhecendo a dificuldade de delimitar o seu verdadeiro conteúdo, escreveram sobre um "*direito ao segredo do ser*"[205] [206].

[201] CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 462, parágrafo II da anotação ao art.º 26.º.
[202] CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 464, parágrafo III da anotação ao art.º 26.º.
[203] Cf. CARVALHO, Orlando de – **Teoria Geral do Direito Civil**. 3.ª ed. Coimbra: Coimbra Editora, 2012, pp. 202*ss*. ISBN 9789723220179.
[204] Daí que se distinga a "identidade social" de "identidade pessoal". Neste sentido, CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 464, parágrafo III da anotação ao art.º 26.º.
[205] CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 468, parágrafo III da anotação ao art.º 26.º.
[206] Não é nossa pretensão delimitar exaustivamente os conceitos "vida privada" e "direito à reserva da intimidade da vida privada". Esta nossa análise, passa antes por escamotear a delimitação do núcleo de proteção de um tal direito na perspetiva que nos interessa: enquadrar a emergência do direito à proteção de dados de forma a percebermos a dinâmica do seu "*momentum*" em contexto de reflexão da eventual "coisificação" dos dados pessoais enquanto bens jurídicos. Por outro lado, perceber o conteúdo do direito à reserva da intimidade da vida privada poderá ser relevante na identificação e compreensão da (in)disponibilidade de determinados bens para circularem no comércio. Sobre o assunto, v. PINTO, P. Mota – **A limitação voluntária do direito à reserva sobre a intimidade da vida privada**. Boletim da Faculdade de Direito. Separata da Universidade de Coimbra (1993), pp. 526*ss*. Este Autor, entende que mais do que distinguirmos diversas "esferas" de vida, importa estabelecer uma "*diretriz geral*" de acordo com critérios objetivos, desde logo, em função de "*valorações de cada formação social*", embora reconhecendo que é caso a caso, pessoa a pessoa, que devemos procurar saber se estamos perante a vida privada de outrem. Não excluímos, por isso mesmo, a possibilidade de a identificação de bens pessoais disponíveis poder passar pela identificação de dados pessoais que, pela sua ligação à dignidade humana e à reserva da intimidade da sua vida privada, à valoração social global, ou à valoração da comunidade em que o indivíduo se insere, não poderão estar na sua disponibilidade para exploração económica. Pense-se, a título ilustrativo, naqueles factos pessoais que, pela sua natureza, estão sujeitos a registo civil e, consequentemente, que carecem de ser publicitados (cfr. com o art.º 220.º-C do Código do Registo Civil) mas que não ficam aquém dos princípios da minimização, da finalidade e da proporcionalidade do seu tratamento (cf. art.º 5.º do RGPD). Em sentido útil, Paulo Mota Pinto refere que não é por determinados "*sinais de identidade*" constituírem factos constantes dos registos públicos que não pertencem à vida privada da pessoa, estando protegidos contra a sua divulgação abusiva – **Direitos de personalidade e direitos fundamentais**. 1.ª ed. Coimbra:

Este quadro de direitos fundamentais, autónomos, não consumíveis entre si, permite-nos indagar sobre o sentido próprio do direito à "*autodeterminação informativa quanto a dados pessoais constantes de ficheiros manuais ou informáticos*"[207] e, em conjugação com o art.º 35.º da CRP76[208], perceber o seu alcance e impacto neste estudo na tentativa da sua conciliação com uma nova realidade que vimos se tem revelado – a da "comercialização" de dados pessoais[209]. Porque mais que um "direito ao nome" temos um dado pessoal, um elemento integrante e identificador da realidade de um sujeito, com uma proteção própria, distinta da tutela do desenvolvimento pessoal tal-qual a enquadramos e "*da* [sua] *protecção como elemento da vida privada*"[210].

O direito à proteção de dados pessoais surge, assim, como um direito de personalidade autónomo e como um direito fundamental que visa proteger bens pessoais, relacionando-se diretamente com a tutela da dignidade da pessoa humana (o seu núcleo essencial e imutável) tal como consagrada na CRP76. Na sua essência repousa um conjunto de posições ativas do titular dos dados, como o direito a conservar informação pessoal longe da invasão de terceiros não autorizados, o direito a definir o âmbito do acesso a essa informação pessoal por terceiros (sejam estes entidades públicas ou privados), o direito a definir e a balizar as condições de tratamento dos seus dados, o direito a conhecer quem tem acesso e em que termos aos seus dados; e, ainda, o direito a manter-se desconhecido pela comunidade. Em suma e nas palavras de Alexandre Sousa Pinheiro, o direito à autodeterminação informativa "*implica todas as possibilidades de um facere, de uma liberdade comunicacional, sem nunca perder a marca d'água originária, ou seja, a defesa contra a intrusão indevida na esfera da personalidade do*

GESTLEGAL, 2018, pp. 530-531. Imaginemos ainda o caso do NIF: este dado pessoal de natureza fiscal não poderia considerar-se vendível. Desde logo, por razões de interesse público, concretamente, de transparência fiscal. Sem prejuízo, não é essa restrição à liberdade de ação do titular sobre os seus dados pessoais que implica que se fale em dados pessoais públicos no sentido de estarem na posse Administração Pública ou no sentido da suprarreferida Lei n.º 10/91.

[207] CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 464, parágrafo III da anotação ao art.º 26.º.

[208] Entende-se que o art.º 35.º da CRP76 visa "*densificar o moderno direito à autodeterminação informacional, dando a cada pessoa o direito de controlar a informação disponível a seu respeito, impedindo-se que a pessoa se transforme em "simples objeto de informações"* (CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 551, parágrafo II da anotação ao art.º 35.º). Como salienta Alexandre Sousa Pinheiro, a "*redacção final do art.º 35.º exprime o conteúdo possível, atendendo ao ambiente político e conhecimentos técnicos difundidos à época*". Esta afirmação serve-nos para enquadrar a forma indireta através da qual "*o texto constitucional português de 1976 foi o primeiro a receber a protecção de dados como "direito"*" (PINHEIRO, Alexandre Sousa – cit., pp. 665 e 681, respetivamente).

[209] Cada vez mais, formas de pagamento não monetárias ganham relevância na aquisição de serviços digitais tidos como "gratuitos", especialmente, através dos dados pessoais transferidos pelos seus utilizadores (titulares de dados pessoais). Cf. GRUNDMANN, Stefan – cit., p. 40.

[210] PINHEIRO, Alexandre Sousa – cit., p. 772.

indivíduo"[211]. Certo é que todos os direitos que cabem aos cidadãos sobre os seus dados pessoais estão associados a um agregado de princípios que vêm sendo igualmente considerados a respeito do tratamento desses mesmos dados. Estes princípios, funcionam como meios e ferramentas legais que visam atribuir o controlo dos dados ao respetivo titular contra, não só o acesso e divulgação indevidos por terceiros, mas, igualmente, a sua centralização, fragmentação ou dissipação de informação indevidos[212]. Afinal, quem melhor que o titular dos dados pessoais para definir o seu destino[213]?

Entendemos que esta questão permite-nos introduzir o tema "*who owns the data*", que se traduz em saber se o controlo atribuído aos titulares sobre os seus dados pessoais permitirá concluir que estes sejam ou possam ser considerados seus proprietários[214], sem prejuízo da eventual necessidade de predefinição de um "núcleo" de dados pessoais que,

[211] PINHEIRO, Alexandre Sousa – cit., p. 810.

[212] Por exemplo, através da interconexão de dados pessoais. Veja-se CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 555, parágrafo VII da anotação ao art.º 35.º.

[213] Christopher Rees entende que os grandes operadores económicos têm tratado os dados pessoais como matéria-prima própria, como se de propriedade sua se tratasse sua, quando tal hipótese deve ser completamente desconsiderada. O que não acontece, desde logo, por a Lei ser incapaz de prover uma resposta convincente e concisa à pergunta "*who owns it?*" [leia-se, "*who owns personal data?*"]. V. REES, Christopher – **Tomorrow's privacy: personal information as property**. International Data Privacy Law [Em linha]. Vol. 3:4 (2013), pp. 220-221 [Consult. 26-08-2019]. Disponível em WWW: <https://doi.org/10.1093/idpl/ipt022>.. No sentido de atribuir um direito de propriedade sobre dados pessoais ao seu titular com o propósito de se lhe conceder o total controlo sobre os mesmos, v. LAUDON, Kenneth C. – cit., p. 97.

[214] No sentido de saber "*whose property it should be*" (ou, em tradução livre, quem deve ser o proprietário dos dados), v. PURTOVA, Nadezhda – **Illusion of personal data as no one's property**. Law, Innovation, and Technology [Em linha]. Vol. 7:1 (2015) [Consult. 10-01-2019]. Disponível em WWW: <https://www.ssrn.com/abstract=2346693>. Segundo esta Autora, não existindo um normativo que identifique a quem estão alocados os dados pessoais "*ab initio*", a grande discussão deve assentar em descobrir o real titular do direito de propriedade sobre dados pessoais e não se sobre os mesmos deve existir um direito de propriedade "*tout court*", partindo do pressuposto que os titulares de tal direito de propriedade são – de facto – os grandes operadores do mercado da Indústria da Informação, pela sua capacidade de recolherem informação pessoal ao nível de "*Big Data*". Em termos práticos, o risco está na dificuldade que os titulares poderão sentir em controlar os seus dados pessoais, uma vez que poderão ver-se na posição de "negociar" a sua privacidade quando a mesma lhes assiste sob a forma de um direito constitucional/fundamental. Parece-nos útil recordar a "*European strategy on the data value chain*" – cit., onde se pode ler sobre a necessidade de o titular não ser prejudicado pela monetização dos seus dados pessoais em prol de uma economia digital europeia, mediante a sua integração no processo de comercialização com dados pessoais sob o seu domínio, e, através de um modelo "*trade-off*", assente na ideia de responsabilização do titular de dados através de informação transparente sobre as possíveis consequências de partilhar os dados pessoais de que é titular com terceiros. Já em 2011, Purtova escrevia a respeito da compatibilidade do regime jurídico da Diretiva de Proteção de Dados com a tutela dos dados pessoais através do regime jurídico da propriedade no contexto europeu, nomeadamente, defendendo que a Diretiva de Proteção de Dados Pessoais, não excluindo a possibilidade do Responsável pelo tratamento de dados pessoais ser titular de direitos de propriedade sobre dados pessoais, teve como grande objetivo atribuir ao indivíduo (i.e., ao titular de dados pessoais), controlo sobre os mesmos. Cf. PURTOVA, N. N. – **Property rights in personal data: A European perspective**. [Em linha]. Oisterwijk: BOXPress BV, 2011, p. 197. [Consult. 04-08-2019]. ISBN 9789088912351. Disponível em WWW: <https://research.tilburguniversity.edu/en/publications/property-rights-in-personal-data-a-european-perspective>.

pela sua "pessoalidade", se considere que não devam estar na disponibilidade do seu titular por ser ilícita a sua circulação no comércio.

Trazemos a este respeito a posição de Václav Janeček[215]. Para o Autor, quando se trata de debater a possibilidade de os dados pessoais serem objeto de propriedade, a informação intrinsecamente pessoal, por ser indissociável da personalidade da pessoa – como por exemplo, o ADN do indivíduo[216] –, seria tutelável ao abrigo dos direitos de personalidade, concretamente, do direito à privacidade. Já os dados pessoais que, segundo Janeček[217], são extrinsecamente pessoais, seriam objeto de propriedade privada e abrangidos pelo respetivo regime jurídico, enquanto objetos legais[218]. Para o efeito, identifica duas abordagens possíveis à introdução deste regime[219], e conclui no sentido de que tal seria perfeitamente compatível com a proteção sobre os dados pessoais e a privacidade que o RGPD pretende instituir. Como método auxiliar a este exercício, poderíamos até analisar as conceptualizações que foram sendo construídas no nosso ordenamento jurídico como a dualidade "esfera pessoal íntima-esfera privada simples"[220].

---

[215] JANEČEK, Václav – **Ownership of personal data in the Internet of Things**. Computer Law & Security Review [Em linha], pp. 1039-1052, pp. 5*ss*. Disponível em WWW: <https://ssrn.com/abstract=3111047>.

[216] Václav Janeček recorre à jurisprudência do Tribunal Europeu dos Direitos do Homem ("TEDH"), concretamente, aos acórdãos Aycaguer v. França, (C-8806/12), de 22-06-2017 e S. v. United Kingdom (C-30562/04), de 4-12-2008. Em suma, em ambos os acórdãos discute-se o equilíbrio entre os interesses em causa (públicos e privados), dada a natureza e a quantidade da informação pessoal que resulta da leitura da descodificação do ADN de uma pessoa. Cf. JANEČEK, Václav – cit., p. 7.

[217] JANEČEK, Václav – cit., p. 8.

[218] Acrescenta aquele Autor: "*Yet ownership protection must relate to personal data qua an ultimate object of ownership rights, and not to personal data qua an intermediary tool of protecting personal information and personality rights*". Cf. JANEČEK, Václav – cit., p. 11.

[219] JANEČEK, Václav – cit., pp. 9*ss*. Sem prejuízo de desenvolvimentos adicionais que a questão suscite, aproveitamos apenas para salientar a existência destas duas abordagens ("*The top down and the bottom-up approach*"), pela sua utilidade no enquadramento deste trabalho. A primeira abordagem justifica a regulação em matéria de propriedade sobre dados pessoais *de jure*, a segunda *de facto*.

[220] Sobre a teoria das esferas da vida privada, v. CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., p. 555, parágrafo VII da anotação ao art.º 35.º; PINTO, P. Mota – cit., p. 524; e, PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais**. 1.ª ed. Coimbra: GESTLEGAL, 2018, pp. 516*ss* e 602*ss*. ISBN 9789895407637. Refletimos ainda sobre a utilidade de distinguirmos "*informação pessoalíssima que integra o "núcleo duro dos dados constitucionalmente tutelados"*" (GUERRA, Amadeu – **Informática e tratamento de dados pessoais – os direitos dos cidadãos e as obrigações dos responsáveis pelos tratamentos automatizados**. Lisboa: Vislis Editores, 1997, p. 63) da demais informação, por referência ao núcleo essencial da dignidade da pessoa humana. Enquadraríamos aqui, por exemplo, aqueles dados cuja colocação no mercado implicaria uma ofensa aos princípios da ordem pública e dos bons costumes, pela sua imensa capacidade de transmitir detalhes do íntimo da pessoa. Pensamos na venda de dados de saúde que indiquem que o titular é seropositivo, como marcadores HIV positivos. A venda de indicadores do estado seropositivo do respetivo titular potenciaria situações discriminatórias como a segregação de indivíduos em larga escala que poderiam impactar a sua vida de forma irreversivelmente negativa. Conseguimos também conceber uma limitação à exploração económica de dados pessoais em função da finalidade do seu tratamento. Imaginamos agora a insuscetibilidade de o titular vender os seus dados pessoais quando o objetivo da compra seja o seu tratamento para fins que possam prejudicar não só o próprio, mas também terceiros.

Assim, quando pensamos em tutela da pessoa relativamente aos seus dados pessoais nesses termos, pensamos no controlo que o titular desses dados precisa de ter sobre os mesmos sob pena de, mais do que desperdícios financeiros, sofrer verdadeiras "crises existenciais" promovidas pela ingerência descontrolada e desmesurada sobre aspetos que integram a sua área de reserva da vida privada[221]. Por outro lado, seríamos imprudentes se ignorássemos a potencial medida em que o direito à proteção de dados pessoais se relaciona com a liberdade de atuação que vem sendo reconhecida à pessoa sobre a sua vida e sobre os seus bens, concretamente, com a sua autonomia privada[222].

4.1. Tangibilidade da privacidade ou usurpação de identidade? O exemplo da exploração económica da imagem

O direito à imagem não só está expressamente previsto no art.º 79.º do C.C. como um direito de personalidade, como a imagem da pessoa é um dado pessoal que pode ser, em função do seu enquadramento, considerado especialmente sensível[223]. O exemplo da exploração económica da imagem comporta, assim, uma componente refletiva de indagação sobre a disponibilidade de "bens" que radicam da personalidade humana, esta, por sua vez, inseparável da personalidade jurídica[224]. Também a tutela que vimos atribuída ao direito à privacidade e ao direito à proteção de dados pessoais no quadro europeu e no quadro constitucional português, tutelados enquanto Direitos Fundamentais, converge, em teoria e por princípio, no caráter dos bens protegidos. Concretamente, bens da personalidade, que, no caso dos dados pessoais, circulam no comércio em benefício do próprio titular ou de terceiros. Ademais, é esta "pessoalidade" dos bens que justifica que, tal como a imagem, também o direito à reserva da vida privada (expressão do "*right*

[221] V. HOOFNAGLE, Chris Jay; WHITTINGTON, Jan – cit., p. 637, nota 114.
[222] No contexto legislativo europeu tem vindo a ser reconhecida a importância da autonomia do indivíduo na gestão da sua privacidade e o dever de os Estados-Membros garantirem os meios necessários à sua proteção, ainda que a Convenção Europeia dos Direitos do Homem ("CEDH") não consagre um direito fundamental autónomo à proteção de dados pessoais ou à autodeterminação informacional. Purtova direciona o tema no sentido do desenvolvimento do direito à privacidade consagrado no artigo 8.º da CEDH, referindo que o percurso jurisprudencial do Tribunal Europeu dos Direitos do Homem ("TEDH") permite ou o germinar de um direito autónomo à proteção dos dados pessoais no quadro da CEDH, ou o seu enquadramento naquele mesmo artigo. Neste seguimento, recorre ao caso do acórdão Reklos e Davourlis v. Greece (processo n.º 1234/05). Nesta decisão, o TEDH reconhece o direito do indivíduo a dispor autonomamente da sua imagem, intrínseco ao seu direito ao livre desenvolvimento enquanto pessoa. Cf. PURTOVA, N. N. – **Property rights in personal data: A European perspective** – cit., pp. 220*ss*.
[223] Nos termos do RGPD, o tratamento da imagem da pessoa, como por exemplo a sua fotografia facial, significará o tratamento de categorias especiais de dados sempre que tais imagens se enquadrem no conceito de dados biométricos – cfr. com o considerando (51) em conjugação com os artigos 4.º(14) e 9.º do RGPD.
[224] CARVALHO, Orlando de – **Teoria Geral do Direito Civil**… – cit., pp. 202-203.

to privacy"[225]) e o direito à proteção de dados pessoais sejam protegidos em sede jus-civilística como direitos de personalidade[226].

Fazemos, assim, a ponte com o tema da eventual "coisificação" dos dados pessoais e, consequentemente, da (im)possibilidade de os mesmos serem passíveis de consubstanciar objeto de propriedade privada. Concretamente, procuramos perceber, se a tendência seria considerar a "objetificação" dos dados pessoais como uma renúncia ao direito de personalidade.

Esta questão foi apreciada várias vezes pelos nossos tribunais a respeito dos contratos de cedência de exploração de imagem de desportistas[227] [228]. Também o sucesso dos "*reality shows*" como o "*Big Brother*" serve de modelo de estudo[229]. Este caso, serve tanto de exemplo no sentido de não estar em causa a denegação da pessoa pela sua "objetificação", como para contrariar absolutismos relativamente à permissão e regulação da participação da pessoa no comércio digital através dos seus dados pessoais. Os participantes destes programas televisivos decidem expor-se – os seus traços físicos e psicológicos que constituem a sua aparência e o seu modo de ser, respetivamente – em função do que consideram adequado ao serviço dos seus interesses particulares, desde logo, financeiros. Os restantes elementos daquela comunidade, tomam igualmente parte de forma interessada e ativa no programa, por exemplo, visitando os seus estúdios, não

[225] Neste sentido, PINTO, P. Mota – cit., pp. 504*ss*; e, PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais**... – cit., pp. 476-477. Ou, de acordo com Orlando de Carvalho, o direito à imagem e o direito à reserva da vida privada são expressões de um direito mais amplo, o "*direito à inviolabilidade pessoal*" (cfr. CARVALHO, Orlando de – **Teoria Geral do Direito Civil**… – cit., pp. 265-266, nota 69).

[226] A ausência de regulação ou previsão expressa no C.C neste sentido não é um fator impeditivo de considerarmos a tutela do direito à proteção de dados pessoais, em sede jus-civilística, no regime jurídico dos direitos de personalidade. O C.C. não apresenta um catálogo fechado de direitos de personalidade, não estamos perante um "*numerus clausus*", e a "*personalidade humana deverá ser protegida pelo direito civil em todas as suas manifestações previsíveis e imprevisíveis*". Vale-nos, desde logo, a cláusula geral do art.º 70.º do C.C., que estipula um "*direito geral de personalidade*" – v. GUIMARÃES, Maria Raquel – **A tutela da pessoa e da sua personalidade como fundamento e objecto da disciplina civilística – questões atuais**. Estudos Comemorativos Dos 20 Anos da FDUP. Coimbra: Almedina. Vol. II (2017), p. 293; PINTO, Carlos Alberto da Mota; MONTEIRO, António Pinto; PINTO, Paulo Mota – **Teoria geral do direito civil**. 4.ª ed. Coimbra: Coimbra Editora, 2005, pp. 209-210 e 212*ss*. ISBN 9723213257*;* e, PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 492*ss*. V. também PINTO, P. Mota – cit., pp. 495*ss*, que nos oferece uma reflexão completa sobre as implicações práticas associadas à sua aplicação e delimitação do direito geral de personalidade ali consagrado no C.C.

[227] Remetemos para GUIMARÃES, Maria Raquel – **A conformação da liberdade contratual pela cláusula geral da ordem pública**. Derecho y autonomía privada: una visión comparada e interdisciplinar, Mª Ángeles Parra Lucán/Silvia Gaspar Lera (diretoras), Granada: Comares, 2017, pp. 426*ss*.

[228] No contexto norte-americano, que vem atribuindo direitos de propriedade sobre a imagem às celebridades, Laudon questiona como poderia a atribuição de tais direitos de propriedade sobre a imagem ser incompatível com as "imagens" que consubstanciem dados pessoais ("*How can a property interest be granted to protect photographic images but not extend to data images?*" Cfr. LAUDON, Kenneth C. – cit., p. 102).

[229] GUIMARÃES, Maria Raquel – **A conformação da liberdade contratual pela cláusula geral da ordem pública** – cit, p. 426.

só por motivos de entretenimento, mas, cremos, também por se relacionarem com os participantes, seus semelhantes. Existe um ganho recíproco entre espectadores-participantes que justifica a existência destes "*reality shows*" e a sua regulação pelo Direito, à semelhança da alienação de dados pessoais.

A alienação de dados pessoais não só não traduz, da nossa ótica, uma *"alienação do direito de personalidade*" respetivo, como optamos por não sustentar a sua ilicitude atendendo à consciência axiológica da comunidade digital que, arriscamos, integra a substancial parte da população europeia e, como vimos, do próprio legislador europeu[230]. Perante o enquadramento da disposição que o titular faça dos seus dados pessoais na tutela dos direitos de personalidade, sempre tenderíamos a considerá-la uma limitação voluntária ao exercício dos seus direitos, seja pelo consentimento[231] seja por acordo[232], ou até, aproximando-nos do entendimento de Paulo Mota Pinto a respeito da "*autodeterminação informativa sobre a vida privada*"[233], uma forma análoga à da "*conformação do objeto do direito pelo seu titular*"[234], e não como uma renúncia ao seu direito à proteção de dados pessoais ou à sua privacidade. No entanto, partindo do pressuposto que estamos perante uma limitação voluntária do direito tal como decorre do art.º 81.º do C.C., o consentimento/acordo do titular para a alienação dos seus dados pessoais sempre cumpriria as exigências do quadro legal em vigor – por exemplo, seria livremente revogável (cf. o n.º 3, do art.º 7.º do RGPD) –, e sempre estaria limitado pelos princípios da ordem pública e dos bons costumes nos termos do art.º 81.º do C.C. conjugado com o art.º 280.º do C.C., que estipula os requisitos do objeto negocial. Aliás, perante esta conceção de que estamos perante um ato permissivo (como o consentimento), do titular, na disposição dos seus dados pessoais, sempre se defenderá a sua revogação

[230] Para maior desenvolvimento sobre o tema, remetemos para PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 705-706.

[231] Paulo Mota Pinto escreve a este respeito que "*além da possibilidade, conferida a cada um, de conformação da própria vida privada (…) as pessoas podem consentir na limitação do direito à reserva nos termos gerais (…) do regime das limitações voluntárias aos direitos de personalidade*". Identificando o Autor, neste seguimento, que o interesse subjacente à tutela da personalidade está condicionado por valorações próprias "*do interessado*, que pode ser motivado pela *consecução de uma vantagem económica como correspectivo direto da limitação*". Cf. PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 565-566.

[232] PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 688-689.

[233] PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 680*ss*.

[234] PINTO, Paulo Mota – **Direitos de personalidade e direitos fundamentais…** – cit., pp. 684*ss*. Dos ensinamentos deste Autor, retiramos que o direito à reserva sobre a intimidade da vida privada distingue-se dos demais direitos "*especiais*" de personalidade pelo facto a "*definição do alcance da sua vida privada*" se fazer de acordo com a vontade do indivíduo em conformar o núcleo da informação sobre a sua vida (privada) que pretende divulgar, a quem, e em que circunstâncias. Esta é uma hipótese de "auto-conformação" do objeto "vida privada" que permite ultrapassar falar-se em limitação voluntária do direito de personalidade através do consentimento do titular seu titular, nos termos do art.º 81.º do C.C.

com fundamento na autodeterminação da pessoa. Seja em função da natureza do ato de aproveitamento do bem, seja em função dos valores neles implicados, seja em função da natureza das concretas razões que o fundamentaram considerando a realidade dinâmica que caracteriza a personalidade de um indivíduo[235]. Decorre, ademais, do próprio RGPD, que a proteção de dados pessoais não é absoluta: veja-se, por exemplo, os considerandos 4 e 18. Por outro lado, entender a alienação de dados pessoais como um poder de disposição que o titular faça sobre os mesmos, à semelhança do poder de conformação do objeto pelo titular do direito como defendido por Paulo Mota Pinto, não prejudica limitarmos essa alienação àquele núcleo de dados pessoais insuscetível de ofender a ordem pública, em termos semelhantes ao que defende Václav Janeček.

Independentemente do entendimento, cremos que o caráter irrenunciável atribuído ao direito à proteção de dados pessoais não prejudica a importância do valor económico conferido aos dados pessoais enquanto objeto de relações jurídicas. Pensamos ainda no chamado "*incentivo ao investimento*" associado ao reconhecimento do "*right of publicity*", tal como configurado no ordenamento americano, numa perspetiva funcional do direito. Este é muitas vezes chamado à colação no tratamento doutrinal da exploração patrimonial da imagem por analogia com a função social do "*copyright*"[236] e, do nosso ponto de vista, perfeitamente admissível no ordenamento jurídico português se atentarmos na função social do Direito de Propriedade Intelectual[237], por exemplo. Por sua vez, a exploração económica de dados pessoais por força da sua "coisificação" poderá contribuir para o reforço da segurança da informação na sociedade digital, funcionando com um incentivo à privacidade enquanto fator de preferência. A privacidade passaria a ser encarada como um fator preferencial pelos titulares dos dados aquando da escolha dos fornecedores de conteúdos e serviços e, estes, por seu turno, preocupar-se-iam em oferecer medidas de segurança mais eficientes e eficazes, não só para se distinguirem pela qualidade dos seus serviços, como pela tutela do seu investimento. Consequentemente,

[235] FESTAS, David de Oliveira – **Do conteúdo patrimonial do direito à imagem – Contributo para um estudo do seu aproveitamento consentido e *inter vivos***. Coimbra: Coimbra Editora, 2009, pp. 187*ss*.
[236] FESTAS, David de Oliveira – cit., pp. 376*ss*.
[237] A criação artística tutelada ao abrigo dos direitos de Propriedade Intelectual não só é a expressão de uma "*liberdade de criação*" (do exercício de um direito de personalidade, portanto), como essa "*autonomia pessoal*" perante o poder público e terceiros é conferida constitucionalmente, e também no plano da promoção de bens culturais (obras, na aceção do Código do Direito de Autor e dos Direitos Conexos ("CDADC" – Decreto-Lei n.º 63/85, de 14 de março). Ademais, o seu núcleo de proteção e a natureza dos bens que a Propriedade Intelectual tem como objeto não impede a sua proteção em sede de direito de propriedade, pelo contrário, faz com que a sua proteção saia "*mais alargada ou reforçada*". Cfr. MIRANDA, Jorge; MEDEIROS, Rui – **Constituição Portuguesa anotada – Tomo I**. 2.ª ed., rev., at. e amp., Coimbra: Coimbra Editora, 2010, pp. 925-926, anotação ao art.º 42.º.

julgamos que testemunharíamos o reforço da privacidade dos titulares dos dados pessoais[238]. Também não é nova a questão da apropriação "*do valor comercial da identidade de uma pessoa"*[239], em que o "retrato" que alguém cria sobre si próprio pode tornar-se uma mais-valia económica, por exemplo, associando o seu nome, imagem, à venda de determinados produtos, tornando-se um sinal distintivo no comércio (i.e., uma marca).

Nesta perspetiva, a alienação de dados pessoais, e uma vez que a imagem da pessoa é também um dado pessoal, poderia igualmente consubstanciar um negócio jurídico sujeito ao regime geral dos negócios jurídicos[240], tendo como especificidade a possibilidade de o titular do dado pessoal poder livremente revogar o seu consentimento[241] [242], em conformidade com o RGPD, sem prejuízo do ressarcimento de eventuais prejuízos causados.

Também não nos parece que a realidade das coisas, como a existência de "*reality shows*" como já referimos, e a troca de bens/serviços por dados pessoais, seja a evidência de termos descurado a sensibilidade da questão. Não se trata de esvaziar a essência do indivíduo e anular a sua privacidade, mas da necessidade de reforçar a tutela dos seus

---

[238] A privacidade dos dados pessoais, por exemplo, numa aplicação de computador, pode ser considerada um parâmetro-chave quando se fala em "*non-price competition*", enquanto critério de qualidade do serviço oferecido. A este respeito, ESAYAS, Samson Y. – **Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law**. *International Data Privacy Law* [Em linha]. Vol. 8:3 (2018), pp. 181–199 [Consult. 20-04-2019], p. 181–199. Disponível em WWW: <https://www.doi.org/10.1093/idpl/ipy014>. O Autor reflete sobre a necessidade de um mercado competitivo para que aquele critério de qualidade de serviço – a privacidade – não seja ilusório, apoiando a sua linha de argumentação em opiniões da EDPS e decisões da Comissão Europeia a respeito de fusões empresariais como Microsoft/ LinkedIn. Esta posição viu-se sustentada na COM(2019) 374 final da Comissão Europeia, de 24-07-2019, da qual decorre que um número considerável de empresas tem promovido o respeito pelos dados pessoais enquanto um fator diferenciador no momento de venda. Sobre o assunto e num mesmo sentido, remetemos ainda a este respeito para Rolf H. Weber em SCHULZE, Reiner; STAUDENNMAYER, Dirk; LOHSSE, Sebastian – **Contracts for the supply of digital content: regulatory challenges and gaps**… – cit., p. 175.

[239] FESTAS, David de Oliveira – cit., p. 196.

[240] Manifestação da autonomia privada da pessoa, corolário do direito contratual civil tal como consagrado no art.º 405.º do C.C.

[241] Além das condições previstas no RGPD para o consentimento – que deve ser livre, esclarecido, específico, inequívoco e livremente revogável (cf. com o art.º 8.º do RGPD) –, uma das formas atualmente não previstas de reforçar o nível de controlo do titular sobre os seus dados pessoais face às bases de licitude para o tratamento dos mesmos (cf. com os artigos 6.º e 9.º do RGPD), seria atribuir prioridade normativa ao consentimento. Isto, sem prejuízo de eventuais exceções/ limitações impostas a tal regra da prioridade normativa do consentimento por razões superiores de ordem pública, ou até privada. Solução que é – note-se – compatível com a tutela dos dados pessoais através do regime jurídico da propriedade. V. PURTOVA, N. N. – **Property rights in personal data: A European perspective** – cit., pp. 195*ss*.

[242] A subjugação dos negócios com dados pessoais ao regime jurídico dos negócios em geral não invalida esta ou outras especificidades que decorrem da particularidade do negócio, de acordo com a liberdade contratual das partes e do próprio regime da proteção de dados pessoais. V. LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Trading data in the digital economy: legal concepts and tools** – cit., pp. 19*ss*.

direitos contra as "forças negras" do mercado[243] mediante a garantia e o reconhecimento jurídicos de que é o mesmo quem dispõe do controlo efetivo sobre a sua informação pessoal. Mostrando-se indispensável contrariarmos a *"tendência para alargar o mercado à personalidade*"[244], é inegável a suscetibilidade prática de os dados pessoais serem avaliados pecuniariamente[245], e, a sua exploração económica, que, embora se traduzindo num negócio de natureza patrimonial[246], não conduz necessariamente a uma situação de usurpação da identidade – seja ela digital ou não. Nesse caso, cremos, sempre teríamos de considerar que o "*objeto*" do direito à proteção de dados a própria pessoa e não os dados *per se*, ao contrário do que viemos referindo e em concordância com Václav Janeček[247] [248]. Pelo exposto, limitamo-nos a apresentar duas faces do mesmo direito de personalidade (pessoal-patrimonial) sem avançar com a autonomização das mesmas, em direitos completamente autónomos.

Alexandre Libório Dias Pereira, parte de uma noção de coisa cuja formulação legal afirma ser "*infeliz*", para defender a "*coisificação* de *certos bens da personalidade*

[243] A respeito da existência de um mercado negro de dados pessoais e do respetivo valor, v. a manchete da "*Forbes Magazine*" em linha de 29-11-2010 (HILL, Kashmir; GREENBURG, Zack O'Malley – **The black market price of your personal info**. *Forbes Magazine* [Em linha]. 29-11-2010. [Consult. 27-04-2019]). Disponível em WWW: <https://www.forbes.com/2010/11/29/black-market-price-of-your-info-personal-finance.html#613b5c641a3d>. Já sob o pretexto de proteção do titular dos dados pessoais e dos utilizadores da Internet contra esse mesmo mercado ("*A global black market for stolen personal data – Cybercriminal underground economies are fueled by one thing — your stolen personal data. Each data type sells for a different price*"), observamos agências a vender soluções tecnológicas que visam o cálculo do valor dos dados pessoais titulados. Veja-se a página de Internet Trend Micro: <https://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/#section-2>. [Consult. 21-06-2021]. E, ainda, a calculadora apresentada pela "*Financial Times*" [Em linha] na sua página na Internet: <https://ig.ft.com/how-much-is-your-personal-data-worth/> [Consult. 03-06-2021].

[244] VASCONCELOS, Pedro Pais de – cit., p. 168.

[245] Sobre o reconhecimento de um direito a conhecer o valor dos próprios dados pessoais, v. p.e., MALGIERI, Gianclaudio; CUSTERS, Bart – **Pricing privacy – The right to know the value of your personal data**. Computer Law & Security Review [Em linha]. (2018). [Consult. 27-04-2019]. Disponível em WWW: <https://www.ssrn.com/abstract=3047257>. Contribuindo igualmente no sentido de preparação do mercado para a regulação de transações que tenham objeto dados pessoais, a "*Digital Asset Trade Association*" ("DATA"), uma organização sem fins lucrativos cofundada por Brittany Kaiser, conhecida por expor alguns dos aspetos que envolveram a atuação da Cambridge Analytica. Ainda neste seguimento, a respeito de um modelo de regulação deste mercado através da adoção de sistemas de gestão de informação e dos seus benefícios para a economia digital e, em concreto, a economia europeia movida por dados, v. LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Trading data in the digital economy: legal concepts and tools** – cit., pp. 349*ss*.

[246] FESTAS, David de Oliveira – cit., pp. 416*ss*.

[247] JANEČEK, Václav – cit., p. 11.

[248] Cremos que a figura dos direitos sobre a pessoa é redutível à possibilidade de se constituírem direitos – não sobre a pessoa – mas, citando: "*sobre distintos modos de ser físicos ou morais da pessoa, ou bens da personalidade, pois o objeto da relação jurídica deve ser sempre um bem*" (cf. PINTO, Carlos Alberto da Mota; MONTEIRO, António Pinto; PINTO, Paulo Mota – cit., p. 339.). No caso que nos ocupa, bens que derivam diretamente da pessoa.

enquanto *"coisas incorpóreas*"[249]. O Autor, reconhecendo, por um lado, que tal coisificação de bens da personalidade não significa a sua imediata redução "*a objectos de direito de propriedade*", e, por outro, a incongruência de se recorrer ao regime jurídico da propriedade para albergar todos os direitos subjetivos, como os direitos sobre informação pessoal ou dados pessoais, admite que "*o legislador parece não se impressionar com isso*". No mesmo sentido foi o artigo 3.º da Lei n.º 12/2005 de 26 de janeiro que regula a "*Informação Genética Pessoal e Informação de Saúde*", segundo o qual "*A informação de saúde (…) é propriedade da pessoa, sendo as unidades do sistema de saúde os depositários da informação*". Notamos ainda que o art.º 9.º do RGPD – concretamente, os números 3 e 4 –, expressamente estatui uma permissão direcionada aos Estados-Membros no sentido de estabelecerem condições próprias em matéria de dados relativos à saúde, dados sensíveis que, segundo "*[a] doutrina, a este respeito, aludia ao "núcleo duro dos dados constitucionalmente tutelados" ou a "informação pessoalíssima*"*"*[250].

4.2. Coisas da Propriedade ou Propriedade das Coisas? Sobre a (des)necessidade de reescrever o Direito de Propriedade

Como confirmamos inicialmente, este trabalho tem como propósito introduzir uma linha de discussão pouco explorada na doutrina portuguesa, na qual procuramos soluções para as questões que vamos levantando:

Qual é a natureza jurídica dos dados pessoais? Qual deverá ser o regime jurídico da sua proteção? Estaremos a ir longe de mais e é esta a origem de um sistema cada vez mais individualista? Em que medida a temática abordada reflete a problemática da decadência da privacidade do utilizador da Internet? Qual o impacto da questão da "coisificação" dos dados pessoais?

Iniciamos a nossa abordagem com base no regime da propriedade privada[251] por entendermos dali resultar a pretensão de equilíbrio entre 3 pontos aparentemente

[249] PEREIRA, Alexandre Libório Dias – **Direitos de autor e liberdade de informação**. (Teses de doutoramento). Coimbra: Almedina, 2008, p. 109.
[250] PINHEIRO, Alexandre Sousa – cit., p. 714.
[251] Nadezhda Purtova escreveu, de forma mais concisa, que existem apenas duas vias para excluir o regime jurídico da propriedade privada do contexto de tutela dos dados pessoais, e que seriam ou o legislador o excluir expressamente do seu âmbito de tutela, ou eliminar os direitos de controlo do titular sobre os seus dados pessoais (retirando-lhe a sua autodeterminação informacional/informativa). Para esta Autora, o regime jurídico da proteção de dados pessoais tal como vinha definido na Diretiva de Proteção de Dados Pessoais era compatível com o regime da propriedade privada tal como reconhecido na maioria dos Estados-membros, por força do efeito "*erga omnes*" atribuído ao titular do direito de propriedade por um lado, e o direito à autodeterminação informacional atribuído ao titular dos dados pessoais, por outro. PURTOVA, N.

incompatíveis: i) a propriedade como a roda motriz de um Estado de Justiça Social e, nesta medida, como um direito que é efetivamente de todos ao mesmo tempo que é de ninguém em particular; ii) a propriedade como o resultado de uma extensão da própria personalidade; designadamente, iii) fruto de um poder de domínio exclusivo sobre "coisas" que integra um património heterogéneo, enquanto aglomerado de direitos sobre bens suscetíveis – ou não – de apropriação pelo seu titular. Ora, a importância destes três pontos está no objetivo que partilham, ou sejam, a satisfação e a proteção da dignidade da pessoa, cuja personalidade é formada dentro de uma sociedade naturalmente configurada por relações interpessoais, de cariz não puramente social.

Na primeira Constituição da República Portuguesa[252], de 1822, o direito de propriedade privada surge codificado no artigo 6.º, que estipulava: "*a propriedade é um direito sagrado e inviolável, que tem qualquer português, de dispor à sua vontade de todos os seus bens, segundo as leis. Quando por alguma razão de necessidade pública e urgente, for preciso que ele seja privado deste direito, será primeiro indemnizado na forma que a lei estabelecer*"[253]. Emerge como um direito (quase) absoluto, expressão máxima de liberdade individual, produto da própria conjetura revolucionária-liberal inspirada na ideia francesa de propriedade como "*prolongamento natural da pessoa*" – nas palavras de Luís A. Carvalho Fernandes[254]. Hoje, a CRP76 prevê, no seu artigo 62.º, um direito genérico à propriedade privada[255] que engloba todos os direitos de conteúdo patrimonial (direitos de crédito, participações sociais, etc.), não se limitando ao "*universo das coisas*"[256]. Fala-se, a este respeito, em propriedade privada em sentido amplo, cuja

N. – **Property rights in personal data: A European perspective** – cit., pp. 187*ss*, 202, 210*ss* e 237*ss*.

[252] Para efeitos de reflexão consideramos a evolução do direito de propriedade privada e a natureza do objeto sobre o qual pode incidir, e não materializamos qualquer pensamento sem que o mesmo tivesse um mínimo de concretização constitucional no sentido da existência de um núcleo fundamental que o legislador ordinário não pode suprimir. Neste sentido, DUARTE, Rui Pinto – **Curso de direitos reais**. 3.ª ed. Cascais: Princípia Editora, setembro de 2013, pp. 361*ss*.

[253] MIRANDA, Jorge – **As constituições portuguesas – de 1822 ao texto atual da constituição**. 5.ª ed. Lisboa: Livraria Petrony Editores, p. 30.

[254] FERNANDES, Luís A. Carvalho – **Lições de direitos reais**. 6.ª ed. Lisboa: Quid Juris, 2009, p. 23. ISBN 9789727244287. V. ainda, MIRANDA, Jorge **– As constituições portuguesas – de 1822 ao texto atual da constituição** – cit., p. 57 relativamente à influência da Revolução Francesa; e, concretamente sobre a Constituição de 1822, pp. 128*ss*.

[255] Quanto à questão de saber se a Constituição determina o conteúdo do direito de propriedade, também FERNANDEZ, Maria Elizabeth Moreira – **Direito ao ambiente e propriedade privada: aproximação ao estudo da estrutura e das consequências das leis-reserva portadoras de vínculos ambientais**. Coimbra: Coimbra Editora, 2001, pp. 172*ss*. ISBN 9789723210231. Nesta sua obra a Autora refere o entendimento maioritário da nossa doutrina, de que a Constituição remete para o legislador ordinário a delimitação do conteúdo do direito de propriedade privada não existindo a predeterminação de um conteúdo constitucional.

[256] CANOTILHO, J. J. Gomes; MOREIRA, Vital – cit., parágrafo II da anotação ao art.º 62.º, p. 800.

razão de ser é "*garantir um espaço de liberdade na esfera jurídico-patrimonial*"[257]. Percebemos, ainda, que os contornos do conteúdo do direito de propriedade surgem tendencialmente ilimitados, e se veem delimitados pelo poder de uso enquanto poder de disposição que o seu titular pode fazer sobre determinado bem apropriável. Que a evolução deste direito subjetivo segue ainda no sentido da sua funcionalização, em proveito não só de interesses comuns e de interesses públicos[258], mas estendendo-se a um conjunto de restrições motivadas por interesses que visam, mais que um fim maior (supra individual), a proteção do núcleo essencial da dignidade da pessoa humana, na veste daquele que, concretamente, participa no tráfego jurídico[259]. É esta a "função social" do direito de propriedade, cujo alcance deve ser procurado no artigo 62.º da CRP76 e, no plano do direito ordinário, no regime do artigo 1305.º do Código Civil. Ora, acompanhando as palavras de Orlando de Carvalho, o direito de propriedade é o "*poder directo e imediato sobre uma coisa, impondo-se à generalidade dos membros da comunidade jurídica e constituindo uma aproximação, derivação ou expressão da forma plena de domínio sobre os bens – com vista a organizar solidariamente as infra-estruturas sócio-económicas dadas*"[260].

O Código Civil enquadra o direito de propriedade no seu Livro III, "Direito das Coisas"; e, o conceito de "coisa" – a sua noção, categoria e natureza –, vem previsto nos artigos 202.º a 216.º do C.C. Numa perspetiva jus-civilista, pode dizer-se que o objeto do direito de propriedade privada, direito real de gozo por excelência, é, antes de mais, uma "coisa", "*aquilo sobre que podem incidir os poderes que caracterizam o direito*

[257] Veja-se a obra de BRITO, Miguel Nogueira de – **Propriedade privada: entre o privilégio e a liberdade**. Lisboa: Fundação Francisco Manuel dos Santos. (Coleção Ensaios da Fundação), 2010, p. 65. O Autor defende que é na CRP76 que devemos procurar se o legislador ordinário respeitou a tutela de um "*espaço de liberdade na esfera jurídico-patrimonial*" do titular do direito.

[258] O artigo 62.º, n.º 2, da CRP76, expressamente prevê que o direito de propriedade cede perante a existência de interesses públicos, originando uma espécie de categoria de limitações ao direito de propriedade, como é o caso da expropriação, da requisição e das servidões administrativas, cujos regimes não cabem no âmbito da nossa análise. Cfr., por exemplo, com os artigos 80.º, 83.º e 88.º da CRP76.

[259] É o caso das relações de vizinhança previstas e reguladas nos artigos 1344.º*ss* do C.C. Sendo, aliás, notória a inserção sistemática do art.º 62.º no capítulo dos direitos e deveres económicos da CRP76, tal não prejudica a sua reconhecida "qualidade" de direito fundamental, análogo aos direitos, liberdades e garantias e, consequentemente, sujeito ao regime do art.º 18.º da CRP76 por via do art.º 17, expressão da "dupla dimensão" dos direitos fundamentais. Neste sentido, nomeadamente, ANDRADE, José Carlos Vieira De – **Os direitos fundamentais na constituição portuguesa de 1976**. 5.ª ed. Coimbra: Almedina, 2012, pp. 108*ss* e 186-187. Isto posto, é nesta perspetiva que inserimos igualmente, nos próximos pontos, a função do Direito de Propriedade Intelectual e do direito à proteção de dados pessoais, bem como a funcionalização do direito de propriedade em prol do Ambiente, crendo que poderá ser útil ao acolhimento da solução legal segundo a qual os dados pessoais são objeto de propriedade.

[260] CARVALHO, Orlando De – **Direito das coisas: do direito das coisas em geral**. Coimbra: Coimbra Editora, 2012, p. 117.

subjetivo"[261]. É o que podemos retirar do artigo 202.º do C.C. que define coisa: "*Diz-se coisa tudo aquilo que pode ser objeto de relações jurídicas*, à exceção das coisas *fora do comércio (...) tais como as que são, por sua natureza, insuscetíveis de apropriação individual*". Nomeadamente e segundo os ensinamentos de Heinrich Hörster, "*não podem ser objeto da relação jurídica (...) as pessoas singulares (...) apesar de ser possível – e o Código Civil assim faz – isolar ou concretizar ou autonomizar certas manifestações da pessoa, tornando estas "objectivações" objecto de direito*"[262].

Grande parte da doutrina portuguesa, tem entendido que estamos perante um "*numerus clausus*", nomeadamente, daquilo que é passível de ser objeto legal do direito de propriedade, e cuja tendência é ser limitado às coisas corpóreas[263]. Neste seguimento, trazemos a reflexão dirigida por Orlando de Carvalho no sentido de se saber se as coisas incorpóreas ou imateriais podem ser objeto de propriedade, e se é possível considerar tais bens (incorpóreos ou imateriais) como "coisas". Para este Autor, da letra do artigo 1303.º do Código Civil decorre que "*o art.º 1303.º não só admite que pode haver propriedade para lá da contemplada no código, como o que chama "propriedade intelectual" (...), mas admite que lhe possa ser estendido, subsidiariamente, o regime que estabelece, o que é dizer, que as admite verdadeiramente como direitos das coisas*"[264]. Recorda o mesmo Autor, que o Código Civil prevê a possibilidade de propriedade sobre direitos, defendendo, em suma, "*que o princípio da coisificação abrange (...) tanto as coisas em sentido estrito* [leia-se, incorpóreas] *como as coisas em sentido amplo (direitos)*"[265]. Vale, ainda, o seu alerta[266], que continua aplicável: "*E é claro que, não tendo o art.º 1302.º, como se prova no texto, a intenção de valer sequer para todo o L. III, relativo ao "Direito das Coisas", e, dada a sua localização no esquema do código, muito menos para todo o direito civil (...)*, importa uma "*interpretação inteligente da lei*" e não uma leitura *"cadavérica"* da mesma, sob pena de se converter num *dogma absolutamente gratuito*". E, a sua crítica[267] sobre a leviandade do legislador em restringir "*o âmbito da propriedade*

[261] Nas palavras de HÖERSTER, Heinrich Ewald na sua obra **A Parte Geral do Código Civil Português: Teoria Geral do Direito Civil**. 5.ª reimpressão da edição de 1992. Coimbra: Almedina, 2009, p. 174. ISBN 9789724007106.
[262] HÖERSTER, Heinrich Ewald – **A Parte Geral do Código Civil português: Teoria Geral do Direito Civil** – cit., p. 175.
[263] Veja-se, por exemplo, ASCENSÃO, José de Oliveira – **A tipicidade dos direitos reais**. Lisboa: Livraria Petrony, 1968, pp. 274*ss*; ASCENSÃO, José de Oliveira – **Direito Civil: Reais**. 5.ª ed. Coimbra: Coimbra Editora Limitada, 1993, p. 38*ss;* e, FERNANDES, Luís A. Carvalho – cit., pp. 30, 47 e 50.
[264] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., p. 145.
[265] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., p. 154.
[266] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., pp. 147 e 148.
[267] Crítica que é reconhecida pelo supracitado Heinrich Höerster na definição de "coisas", não obstante a

civil às coisas corpóreas, pois, além de não constituir qualquer risco para as propriedades sui generis, (cuja regulamentação especial sempre primaria sobre a regulamentação geral), a solução inversa obstaria a que, como no caso do estabelecimento, se suscitassem dúvidas, enquanto a regulamentação especial não existe, sobre a aplicação aos bens em jogo de princípios que de nenhuma forma dependem da corporalidade e simplicidade do objeto: nomeadamente, os dos arts. 1305.º a 1315.º(...)"[268]. Sendo, atualmente, o regime da transmissão do estabelecimento comercial assunto amplamente discutido e solidamente tratado na jurisprudência, essencial é mantermos em consideração o perigo de cairmos numa realidade em que os tribunais "*a pretexto da observância da lei, coonestam ilegalidades gritantes*"[269]. Também Rui Pinto Duarte nos diz, em "O ensino dos direitos reais", que "*Do art.º 1302.º não é legítimo retirar que o direito de propriedade só pode ter por objeto coisas corpóreas. É ao intérprete que cabe retirar conclusões quanto aos objetos possíveis do conceito doutrinário de propriedade*; e que, "*Dos art.º 1302.º e 1303.º também não se pode retirar que os direitos de autor e a propriedade industrial não são direito de propriedade. (...) Do art.º 1302.º não se pode outrossim retirar que os demais direitos reais não podem ter por objecto coisas incorpóreas*"[270].

Isto posto, consideramos que o ambiente "*de facto*" que viemos refletindo pode justificar interpretações criativas da nossa Lei vigente, e que não implica necessariamente reescrever o regime do direito de propriedade. Nesta ordem de razão, as alterações introduzidas pela Lei n.º 8/2017, de 3 de março, ao Livro III do C.C., refletem, cremos, as posições doutrinais suprarreferidas, sem prejudicar o resultado interpretativo que pretendemos introduzir.

4.3. Um (outro) novo paradigma do Direito de Propriedade? Sob a perspetiva do regime jurídico do animal à luz das alterações introduzidas pela Lei 8/2017

Sob a epígrafe "*Objeto do direito de propriedade*", o n.º 1 do artigo 1302.º do C.C. com as alterações introduzidas pela Lei n.º 8/2017, de 3 de março, define que as coisas corpóreas podem ser objeto de propriedade tal como regulado naquele diploma. A redação anterior deste artigo, dada pela versão original do DL n.º 47344/66, de 25 de novembro,

sua posição de que as coisas incorpóreas não podem ser objeto de propriedade privada.

[268] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., p. 148.

[269] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., p. 148.

[270] DUARTE, Rui Pinto – **O ensino dos direitos reais propostas e elementos de trabalho**. Lisboa: Coimbra Editora, 2004, pp. 28 e 29.

previa que "*Só as coisas corpóreas (…) podem ser objeto do direito de propriedade regulado neste código*" (sublinhado nosso). As alterações substancialmente relevantes, não estão associadas apenas à eliminação do advérbio de exclusão "só", mas ainda na utilização do advérbio "também", usado para estabelecer a continuidade expressa no n.º 2 do mesmo preceito. Notória é identicamente a evolução do pensamento político e filosófico no sentido de aceitar e reconhecer o animal como um ser vivo dotado de sensibilidade, com dignidade própria, e cuja condição biológica deve ser respeitada por forma a se potencializar a sua existência condigna e natural. O facto de a justiça que o Direito pretende salvaguardar não ser perfeita, deriva de o seu criador também não o ser. Sendo visível o progresso de uma conceção meramente utilitarista do animal para uma visão pró-animal, efeito útil de uma imposição da ética e da moral vigente sobre o Direito, interessa-nos que, agora, não só as coisas possam ser objeto do direito de propriedade como também os animais. Porém, associada a esta alteração de pensamentos e de regimes, está a problemática subjacente à classificação dos animais: se não são "coisa", são o quê?[271] Ora, se do ponto de vista do conteúdo patrimonial do direito de propriedade o animal pode ser objeto de relações jurídicas, sustentar a possibilidade de um bem jurídico-ambiental ser objeto de propriedade privada traz um momento de rutura face à tradicional conceção de que só as "coisas" – independentemente da sua (i)materialidade – poderem ser objeto de propriedade.

4.4. Um direito especial de propriedade? A ponte com o Direito de Propriedade Intelectual

Ainda no sentido da desnecessidade de reescrever a terminologia usada no artigo 1303.º do C.C., voltamos a Alexandre Libório Dias Pereira, que considera a possibilidade de direitos de propriedade terem como objeto coisas incorpóreas, ainda que se vejam regulados em legislação especial[272]. Nestes seus estudos, o Autor transporta a "*índole fragmentária da noção de propriedade*"[273], que permitirá um jogo de cintura entre os princípios tradicionais subjacentes à *propriedade civil* e os princípios então emergentes,

[271] "Coisa" e "objeto de relações jurídicas" não são equivalentes, diferentemente do que parece resultar do art.º 202.º do C.C. – "*nem tudo o que é susceptível de ser objeto de relações jurídicas é uma coisa em sentido jurídico*". Cf. PINTO, Carlos Alberto da Mota; MONTEIRO, António Pinto; PINTO, Paulo Mota – cit., pp. 219*ss* e 344*ss*. Os direitos sobre os animais integram o património da pessoa enquanto direitos de propriedade, património que, por sua vez, pode ter como objeto direitos sobre bens jurídicos distintos das coisas.
[272] PEREIRA, Alexandre Libório Dias – cit., pp. 95*ss* e 166*ss*.
[273] PEREIRA, Alexandre Libório Dias – cit., p. 97.

desde logo, face à "*elasticidade daquele direito e* [à] *função social que as leis modernas lhe atribuem*"[274].

O objeto do Direito de Propriedade Intelectual é tendencialmente reconhecido na doutrina portuguesa como sendo uma "coisa incorpórea"[275], reconhecendo-se, consequentemente, que estamos perante uma verdadeira forma de Propriedade[276] [277], compreendendo-se as "*obras de engenho*" como produtos do intelecto tuteláveis uma vez autonomizadas da sua "*personalidade criadora*" e, assim exteriorizados[278], passíveis de serem "coisas"[279]. Recorrendo novamente às palavras de Orlando de Carvalho: "*uma vez que a noção ampla de coisa é a única "que corresponde à verdadeira função do Direito, cujo objeto não é ordenar fisicamente o mundo dos corpos, mas ordenar socialmente a comunidade, em que os direitos, estabelecimentos e energias têm o mesmo valor funcional das coisas corpóreas""*"[280]. Este mesmo Autor, reconhecendo a eventual aversão ao conceito de "coisas incorpóreas", mantém-se fiel à ideia de que "coisas" são autênticas "*fontes de interesses*" e de que é esse facto que permite caracterizá-las como tal: "*Só há coisas onde há interesses conflituantes e são coisas tudo o que suscita conflitos que podem vir a resolver-se num aproveitamento directo*"[281].

Nesta senda, na doutrina estrangeira, Sjef van Erp, num estudo publicado pela Universidade de Maastricht, analisou a possibilidade de os dados pessoais serem entendidos como objeto legal do direito de propriedade, precisamente por também os dados pessoais terem uma natureza não-física (i.e., intangível). Face à então recente versão do parágrafo 2 do art.º 567.º do Código Comercial luxemburguês que visou refletir a possibilidade de reivindicação da propriedade sobre dados por quem reclama o seu controlo, Sjef van Erp abordou o tema questionando a possibilidade de a informação se

[274] VARELA, Antunes; LIMA, Pires de – **Código Civil – Anotado**. Vol. III, Artigos 1251.º a 1575.º, 2.ª ed. reimpressa. Coimbra: Coimbra Editora, 2010, pp. 84 e 85.
[275] Neste sentido, CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., p. 140.
[276] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., pp. 144 e 145.
[277] Também Pires de Lima e Antunes Varela abordaram esta questão, partindo do pressuposto de que o legislador sistematizou a "Propriedade Intelectual" no Capítulo da "Propriedade em geral" do C.C., concretamente, no artigo 1303.º, com o objetivo de resolver a natureza jurídica do Direito de Autor. Cf. VARELA, Antunes; LIMA, Pires de – cit., pp. 86 e 87.
[278] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., pp. 144 e 145. Interpretação, no mais, consonante com o artigo 1.º, n.º 1 do CDADC.
[279] Cfr. PINTO, Carlos Alberto da Mota; MONTEIRO, António Pinto; PINTO, Paulo Mota – cit., pp. 219*ss*, 336*ss* e 341*ss*. Para estes Autores, um direito (como o direito de autor) pode recair sobre coisas incorpóreas ou bens imateriais que, inclusive, têm um valor patrimonial autónomo.
[280] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., pp. 141 e 142.
[281] CARVALHO, Orlando de – **Direito das coisas: do direito das coisas em geral** – cit., pp. 134 e 135.

autonomizar do seu "portador" e, naturalmente, a constituição de direitos de propriedade sobre os dados através da sua transformação no mundo físico (um exemplo seria através da sua inclusão numa PEN USB)[282].

Quanto a nós, sobre a existência de abertura legislativa nacional para acolher a tutela jurídica dos dados pessoais como coisas incorpóreas, através de um regime (especial) de propriedade, propomos o seguinte exercício lógico:

i) Os dados pessoais traduzem qualquer característica – física, fisiológica, psicológica, cultural, social, económica, etc. –, capaz de identificar, de alguma forma, dentro da razoabilidade do contexto, uma pessoa natural;
ii) Têm na sua génese o desenvolvimento da personalidade da pessoa, enquanto derivação do ser;
iii) A sua "materialização" consiste e depende da sua transformação em existência física; e,
iv) Está dependente de um processo de extração/recolha promovido ou não por terceiros;
v) Tal "materialização" é o reflexo da autonomização dos "bens" da pessoa em causa – os seus dados pessoais –, que se tornam apropriáveis e objeto de domínio.

5. Discussão final e conclusão

Aqui chegados, vimos que é inegável a existência de um mercado de dados pessoais, e a Diretiva (EU) 2019/770 representa uma assunção disso mesmo por parte do legislador europeu[283]. Ademais, a recente Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à governação de dados (Regulamento Governação de Dados)[284] vem reforçar isto mesmo, quando enquadra o processamento de dados pessoais como necessário na criação de cadeias de valor[285], reconhecendo que o regime que pretende

[282] Fê-lo de novo recentemente, debatendo a necessidade de se discutir a criação de um regime privado próprio para a proteção dos dados pessoais enquanto um bem monetizável do seu titular, em LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Data as Counter-Performance – Contract Law 2.0?** – cit., pp. 83*ss*.

[283] Neste sentido também Sjef van Erp em LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Data as Counter-Performance – Contract Law 2.0?** – cit., pp. 84*ss*.
[284] COM(2020) 767 final.
[285] Quanto ao seu texto, nossa crítica segue, antes de mais, para o facto de este Regulamento de Governação

introduzir foi concebido de forma a respeitar "*plenamente a legislação em matéria de proteção de dados*" e a aumentar *"o controlo das pessoas singulares sobre os dados que geram*".

Assente nesta ideia de viabilizar o controlo efetivo dos dados pessoais, pelos seus titulares, concretamente, no contexto da sua inclusão no comércio jurídico, procuramos analisar o seu enquadramento no regime jurídico vigente e a necessidade de o adequar em conformidade com a realidade prática do mercado, desde logo, concebendo a introdução de um novo objeto legal de propriedade, os dados pessoais, sem que tal implique, como viemos defendendo, desrespeitar o RGPD. Nomeadamente, através da consideração dos dados pessoais como "coisas", passíveis de ser objeto de propriedade (reforçamos, ainda que tutelados por via de um regime jurídico especial). Por um lado, concebemos que o património da pessoa é constituído por direitos sobre bens de diversas razões e ordens[286] suscetíveis de regular a posição do proprietário, princípio central da lógica da sua funcionalização; por outro lado, demonstrado o interesse que a valorização dos dados pessoais no mercado desperta nos operadores económicos, compreendemos aquela doutrina que vem defendendo o "*pluralismo dominial*". Segundo este entendimento, a "*situação jurídica do proprietário (o conteúdo da propriedade) varia em função da natureza e objeto sobre o qual a propriedade incide*"[287]. Esta referência importa-nos ainda pela "pessoalidade" enquanto elemento intrínseco de um dado pessoal – os dados pessoais derivam, naturalmente, de uma pessoa, um sujeito determinado, caracterizado por uma personalidade própria, única, que o individualiza. "*Maxime*", questiona-se se será possível que algo que não nasce necessariamente da pessoa, mas que decorre da sua existência, os seus dados pessoais, possa ser objeto de propriedade. E, então, quais seriam os princípios da "propriedade em geral" e os aspetos do seu regime a aplicar à propriedade sobre dados pessoais, e onde residiria a especialidade do seu regime.

---

de Dados, embora reconhecendo a necessidade de atribuição aos cidadãos de controlo sobre os dados pessoais por si gerados, salvaguarda essencialmente o capital das empresas (como o seu investimento na recolha dos dados) no processo de monetização dos mesmos.

[286] Enquanto produto de Direito, o direito de propriedade privada, quando corretamente delimitado, reflete a sua coerência com todas as normas do ordenamento jurídico sejam elas de natureza pública ou privada. V. p.e., BRITO, Miguel Nogueira de – cit., pp. 67*ss*.

[287] FERNANDEZ, Maria Elizabeth Moreira – cit., p. 170*ss*.

Procurou-se explorar algumas particularidades destas interrogações ao longo deste artigo e são já várias as contribuições por parte de diversos autores que participam na discussão[288]. Por ora, parece-nos interessante considerar, por exemplo, o cenário de doação de espermatozoides, em que podemos questionar o anonimato do doador[289] e,

[288] P.e. Sjef van Erp salienta no estudo supracitado os requisitos da especificidade e da publicidade subjacentes ao princípio da transparência do Direito de Propriedade: de acordo com o Autor, se a informação não é de alguma forma passível de ser claramente descrita e delineada, se o titular não for capaz de a fazer valer, como sua, contra terceiros, então a mesma informação não é suscetível de ser objeto legal de propriedade. Para o efeito, indica 3 elementos úteis na hora de determinar se a informação pode ser específica o suficiente para ser considerada objeto de propriedade: i) a natureza do seu conteúdo, ii) a pessoa que cria o conteúdo, iii) e o propósito e uso do conteúdo. V. VAN ERP, Sjef J. H. M – cit., pp. 12*ss*. Já Gianclaudio Malgieri, apercebendo-se do circunstancialismo que rodeia a economia digital, em que os dados pessoais são objeto de monopólio, escreve sobre as vantagens do regime do segredo comercial perante os desafios relacionados com a apropriação de dados de clientes, pelas empresas. Para este Autor, os dados pessoais seriam uma espécie de segredo comercial das pessoas, seus titulares, que deles podiam dispor através de licenças comerciais. As empresas criariam políticas personalizadas (por exemplo, de "*marketing*" ou privacidade) que permitiriam ao consumidor partilhar, através de licenças, os dados pessoais que desejasse. Tal hipótese permitir-lhes-ia aceder, ainda que em proporção dos dados fornecidos, aos serviços e/ou bens das daquelas empresas. Por sua vez, as dificuldades associadas por muitos à "coisificação" dos dados pessoais, como a definição de um valor dos dados ou a quebra do mercado pela perda de capacidade competitiva de pequenas e médicas empresas, seria ultrapassada com a adoção do regime da "*quasi-property*" da "*common law*". Portanto, uma solução através de um regime jurídico orientado para a propriedade privada, preferencialmente, seguindo os ensinamentos de Paul Schwartz. Soluções de regime como o do segredo comercial têm sido consideradas por várias ordens de razão. Quer para permitir ao titular dos dados pessoais manter determinado nível de controlo sobre os mesmos, quer para, simultaneamente, possibilitar a sua comercialização sem maiores entraves e balanceando a assimetria da posição do titular e o grande operador do mercado. Nesta sequência, o licenciamento de dados pessoais acarretaria para o titular, designadamente, um meio de limitar o seu tratamento a outra finalidade que não a definida na licença, fomentando, assim, o seu secretismo. A doutrina que defende tal tese, como Malgieri, acaba por sustentar a sua posição relativamente ao licenciamento no art.º 17, n.º 2 do RGPD. V. MALGIERI, Gianclaudio – **'Ownership' of customer (big) data in the european union: Quasi-property as comparative solution?** Journal of Internet Law [Em linha]. Vol. 20:5 (2016) [Consult. 27-04-2019]. Disponível em WWW: <https://www.ssrn.com/abstract=2916079>. Do mesmo Autor, MALGIERI, Gianclaudio – **Trade secrets v personal data: a possible solution for balancing rights**. International Data Privacy Law [Em linha]. Vol. 6:2 (2016) 102–116 [Consult. 4-05-2019]. Disponível em WWW: <https://www.doi.org/10.1093/idpl/ipv030>. V. ainda, SCHWARTZ, Paul M. – **Property, privacy, and personal data**. Harvard Law Review [Em linha]. Vol. 117, Vol. 7, (2004) 2055*ss* [Consult. 27-04-2019]. Disponível em WWW: <https://www.ssrn.com/abstract=721642>; não obstante a doutrina deste Autor não ser totalmente compatível com o ordenamento jurídico português, tal como Orlando de Carvalho que, como vimos, defende que estamos perante coisas quando as mesmas suscitam conflitos derivados de interesses direcionados que podem vir a resolver-se num aproveitamento direto, Schwartz defende que, tal como o tradicional direito de propriedade sobre determinado objeto, a propriedade sobre informação pode ser caracterizada como um agrupamento de interesses. Embora muitas das ideias adiantadas por Paul Schwartz estejam já refletidas no texto do RGPD, pela complexidade da natureza do regime de tutela dos dados pessoais torna-se necessário maior debate e investigação sobre o tema, o que ora também se pretende instigar. Em todo o caso, entendemos que o RGPD não barra a possibilidade de um modelo de propriedade sobre dados pessoais. É igualmente neste sentido que Malgieri introduz na discussão a "*quasi-property*" que, segundo o Autor, ajudaria a colmatar as objeções à "coisificação" de bens estritamente relacionados com a natureza humana. Nomeadamente, através de um regime próximo do da propriedade, mas dotado de efeitos "*inter partes*", típicos dos direitos pessoais: o titular teria o direito de apenas excluir o tratamento dos seus dados pessoais por determinadas entidades, para determinados fins, com certos propósitos e dependendo até do grau de relacionamento entre as partes.

[289] É interessante atentar, por exemplo, no guia da Autoridade de Controlo Inglesa (Information Commissioner's Office – "ICO") onde são explorados os riscos de re-identificação dos titulares dos dados, "*Anonymisation: managing data protection risk code of practices*" [Em Linha]. Consult. 02-06-2021.

consequentemente, se estamos a potenciar, em última linha, o fornecimento de dados pessoais genéticos (informação de saúde e genética, dados especiais nos termos do artigo 9.º do RGPD e, vimos, propriedade da pessoa nos termos da Lei n.º 12/2005, de 26 de janeiro). Daqui, poderíamos investigar vários aspetos do regime aplicável a este ato nos vários países europeus com o intuito de analisar o seu impacto na ótica da proteção dos dados pessoais e, especialmente, da sua circulação no tráfego jurídico, desde o ressarcimento ou pagamento ao titular dos dados, à gestão de um banco de dados, e, em especial: i) o âmbito do próprio conceito de dados pessoais; e, ii) o impacto do processamento (dir-se-á inconsciente) de dados em relação a terceiros ao seu titular (diremos, primário). No primeiro ponto, indagaríamos sobre se o esperma de um doador poderia ser considerado dado pessoal na aceção do artigo 4.º, alínea 1) do RGPD, ou, e assim cremos, um suporte de informação. Sendo certo que o conceito de dados pessoais tem sido considerado amplamente tanto pela doutrina como pela jurisprudência do Tribunal de Justiça da União Europeia, entendemos que para esta discussão poderá contribuir, analogamente, a posição de M. R. Leiser e Francien Dechesne relativamente à (des)consideração dos modelos de "*machine learning*" como dados pessoais[290]. A respeito do segundo ponto, reportamo-nos à teoria do "*network effects of individual privacy choices*"[291], que defende a atribuição de um direito de propriedade coletiva sobre os dados pessoais em detrimento de um direito de propriedade individual, face ao impacto das escolhas de um titular (diremos novamente, primário) a respeito do processamento dos seus dados pessoais, para o exemplo, dados genéticos, na autodeterminação informativa de terceiros, preconizando, assim, uma privacidade de grupo.

Disponível em WWW: <https://ico.org.uk/media/1061/anonymisation-code.pdf>. E, recentemente, o seu novo guia (ainda em raschunho), "*Draft anonymisation, pseudonymisation and privacy enhancing technologies guidance*" [Em Linha]. Consult. 03-06-2021. Disponível em WWWW: https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>. Também a Comissão Nacional de Proteção de Dados ("CNPD"), no seu Parecer PAR/2021/58, em particular no ponto "*ii. Os dados anonimizados e o risco de re-identificação dos seus titulares*". Consult. 03-06-2021.

[290] V. M R Leiser; Francien Dechesne – **Governing machine-learning models: challenging the personal data presumption**. International Data Privacy Law, Volume 10, Issue 3, august 2020, pp. 187-200.

[291] V. PURTOVA, Nadezhda - **Do property rights in personal data make sense after the Big Data turn? Individual control and transparency.** Journal of Law and Economic Regulation [Em Linha]. 10(2) (novembro 2017), pp. 12*ss.* [Consult. 02-06-2021]. Disponível em WWW: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3070228>.

Este entendimento é ainda pertinente quando nos focamos na conceção dos dados pessoais enquanto objeto legal face aos recentes desenvolvimentos de Sjef van Erp[292], que introduz a ideia de "gestão de dados", ou, talvez, diríamos, "administração de dados", em particular, quando além de um direito de privacidade de grupo, Purtova aclama uma "*gestão coletiva de dados pessoais*"[293]. Segundo Sjef van Erp, poderemos ter outras partes envolvidas nessa gestão de dados pessoais e dela beneficiárias, além do titular dos dados pessoais, designadamente, o responsável pelo tratamento dos dados pessoais e o subcontratante na aceção do RGPD.

Neste seguimento, e em tom de contribuição, parece-nos igualmente pertinente o exercício de cruzar as figuras de "intermediário de dados", "detentor de dados" e "utilizadores de dados" introduzidas na Proposta de Regulamento Governação de Dados, bem como a terminologia ali usada (veja-se, por exemplo, o artigo 3.º, "*(1) O presente capítulo aplica-se aos dados na <u>posse</u> de (...).*" – sublinhado nosso), com o desenho e a construção de um mercado regulado. A este respeito, em 1996, Kenneth Laudon partia da premissa de que a privacidade do indivíduo seria salvaguardada se lhe atribuíssemos direitos de propriedade sobre a sua informação pessoal, a par da criação de um Mercado Nacional de Informação ("*National Information Market*" ou "NIM") através do qual os titulares de tais direitos de propriedade poderiam ser devidamente compensados pelo uso – por terceiros – da sua informação pessoal[294]. A ideia é a de que o enquadramento dos dados pessoais no regime de propriedade privada terá de assumir uma evolução face aos (pré)conceitos jurídicos a respeito do direito de propriedade, desde logo, refletindo uma noção "*fluída*" deste direito, a tal noção de "*pluralismo dominial*", associada à conceptualização da titularidade sobre um património heterogéneo que os dados pessoais podem integrar. Traduzindo as palavras de Purtova[295], a característica maior do direito de propriedade tal como entendido nos vários ordenamentos jurídicos europeus e que

[292] Em LOHSSE, Sebastian; SCHULZE, Reiner; STAUDENNMAYER, Dirk – **Data as Counter-Performance – Contract Law 2.0?** – cit., pp. 90*ss*.
[293] V. PURTOVA, Nadezhda - **Do property rights in personal data make sense after the Big Data turn? Individual control and transparency** – cit., p. 18.
[294] LAUDON, Kenneth C. – cit., pp. 93 e 99*ss*.
[295] V. PURTOVA, Nadezhda - **Do property rights in personal data make sense after the Big Data turn? Individual control and transparency** – cit.

possibilitará ao titular um maior controlo efetivo sobre os seus dados pessoais, é o facto de ser considerado um interesse legalmente tutelado sobre um objeto, seja ele tangível ou não, oponível "*erga omnes"*.

Resta-nos apelar a que ambiguidade do tema não seja um elemento dissuasor de maior discussão. A economia digital atual é impulsionada pelo facto de os utilizadores da Internet das Coisas e, também, consumidores, alienarem os seus dados pessoais por oposição ao pagamento de um preço, no âmbito de fornecimento de conteúdos e serviços digitais. Esta realidade, resultado da monetização que os operadores do mercado fazem dos dados pessoais, põe em causa o controlo que o respetivo titular tem sobre os mesmos dados. O quadro legislativo europeu, não obstante os seus normativos, cada vez mais conscientes em matéria de proteção de dados pessoais e de defesa do consumidor, teve origem num ideal de mercado único que impõe a livre circulação de dados. As preocupações comunitárias não se cingem, assim, à defesa do direito fundamental da pessoa à proteção dos seus dados pessoais, mas estão igualmente direcionadas à procura do equilíbrio da sua proteção com a sustentação e sustentabilidade de uma economia digital europeia, cuja base é a atribuição de valor aos dados através da criação de uma cadeia de valor. Este novo tipo de mercado tem afetado a evolução da economia em geral, que se diz cada vez mais digital, e, perante a ausência de um corpo normativo robusto e maduro capaz de especificamente regular os aspetos mais particulares da alienação de dados pessoais, o titular de dados pessoais vê-se prejudicado em várias frentes:

i) Ao nível da sua economia pessoal: o titular não consegue calcular o valor dos seus dados pessoais e, consequentemente, está sujeito à livre regulação do mercado pelos grandes operadores económicos;
ii) Ao nível da sua privacidade: o titular de dados pessoais não consegue reivindicar o carácter privado da sua informação, cabendo-lhe um défice de poder de controlo sobre a mesma em virtude do poder económico dos grandes operadores do mercado e da falta de um modelo de governo capaz;
iii) Ao nível da sua vida social: o titular de dados pessoais cujo poder de controlo sobre os mesmos é deficitário está sujeito a que o seu perfil – desenhado, por exemplo, através dos seus hábitos e consumos e tendo por base algoritmos opacos e falíveis – esteja na disponibilidade de um maior núcleo de indivíduos;
iv) Ao nível da sua vida económico-familiar: o titular de dados pessoais cujo perfil financeiro se vê discriminado por uma entidade de crédito que recusa financiar a sua morada de família; e, a tantos outros níveis.

Em suma, o titular de dados pessoais vê-se prejudicado ao nível do seu desenvolvimento enquanto pessoa, por lhe ser ditado todo o seu percurso de vida sem que disso se aperceba ou beneficie com toda a justiça ao seu alcance.

É, neste sentido, perante as injustiças promovidas por um mercado desregulado, que acreditamos que a conceptualização dos dados pessoais, enquanto bens da personalidade, deve ser ultrapassada e, talvez, pela sua "coisificação". Sendo discutível qual o regime jurídico que melhor serviria o titular dos dados pessoais, perante este cenário, vemos como várias as possibilidades embora atualmente desajustadas às necessidades práticas de tutela. Como tal, uma busca pelos atributos mais pertinentes de regimes jurídicos que confiram ao titular uma forma de controlo sobre os seus dados pessoais, como o da Propriedade Privada, serviria ao desenho de um regime especial que salvaguardasse a exploração económica de dados pessoais, cuja especialidade decorreria das imposições do próprio regime de proteção de dados pessoais vigente, mas também das particularidades do seu âmbito de aplicação. Esta solução primaria pela sensibilização do jurista português para um cenário prático, reconhecidamente atual, mas que vê o alcance das suas problemáticas limitado pela defesa de um direito de personalidade.

II_Outros Estudos

Proteção e Tratamento de Dados Pessoais de Jogadores Online

Francisco Carvoeiras[296]

RESUMO

O texto apresentado respeita aos jogos *online* e à legislação aplicável, bem como as matérias de proteção de dados com eles relacionados. São, também, mencionadas as regras de seguranças envolvidas nesta atividade.

PALAVRAS-CHAVE

Jogos *online*, transparência, segurança, inspeção, jogo compulsivo.

[296] Licenciado em Engenharia, mestrando em Engenharia de Segurança Informática no Instituto Politécnico de Beja.

Data Protection and Processing on personal data of Online Players

RESUMO

This paper concerns to online games, to the law applicable and the issues of data protection envolved. The paper also mentioned the security rules used.

KEYWORDS

Online games, transparency, security, inspection, compudsive game

Introdução

Os jogos de apostas e os chamados jogos de azar são uma realidade que nos acompanha há muitos anos, sendo um dos exemplos mais conhecidos os casinos. Com a evolução tecnológica e a massificação do acesso à Internet, os casinos e casas de apostas *online* tornaram-se também uma realidade, permitindo a grande parte da população mundial ter acesso facilitado a este tipo de jogos, quer utilizando um computador, um *tablet* ou até um s*martphone*, tudo dispositivos que fazem parte do nosso quotidiano.

1. Base legal

Em Portugal, o jogo *online* carecia de regulamentação até que surgiu o Decreto-Lei nº. 66/2015, de 29 de abril, baseando-se nas melhores práticas adotadas com sucesso noutros países há vários anos e indo de encontro às recomendações da União Europeia.
Conforme mencionado no Art.º 9.º da Secção I do Capítulo III, o direito de explorar os jogos e apostas *online* é reservado ao Estado, sendo cometidas as competências de controlo, inspeção e regulação de jogo *online* a nível nacional à Comissão de Regulação e Inspeção de Jogos do Turismo de Portugal.

Esta regulação pretende que os operadores e jogadores nacionais passem a atuar de forma mais transparente, combatendo uma economia paralela e informal, evitando-se a fraude e o branqueamento de capitais e combatendo a viciação de jogo e resultados através da proibição de jogo de qualquer pessoa que tenha possibilidade de acesso aos sistemas informáticos dos jogos ou pessoas que possam ter intervenção direta ou indireta nos resultados dos eventos, tais como árbitros de futebol.

Pretende-se ainda estimular a cidadania e a proteção de menores e pessoas mais vulneráveis, tais como membros do Governo (pela sua exposição), e jogadores compulsivos (pela sua fragilidade decorrente dessa condição).

Por este motivo, tem de haver uma especial atenção à forma como são tratados os dados dos jogadores por parte das entidades exploradoras, devendo existir estritas políticas de proteção de dados. Neste aspeto saliente-se desde logo que, não existindo um regime específico para o jogo *online*, é aplicável de modo geral o disposto no RGPD, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

Remetem para isso mesmo o n.º 1 do Art.º 93.º do Decreto-Lei 66/2015: "O disposto no RJO não prejudica a aplicação a todas as atividades por ele abrangidas da legislação em matéria de proteção de dados pessoais, nomeadamente a Lei n.º 67/98, de 26 de outubro, e a Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, incluindo no que respeita ao exercício dos direitos pelos titulares dos dados e ao regime de acesso de terceiros, em tudo o que não seja legitimado pelo presente regime.", e o n.º 2 do mesmo Artigo: "As entidades envolvidas nos jogos e apostas online, incluindo as entidades exploradoras e a entidade de controlo, inspeção e regulação, estão sujeitas ao cumprimento dos princípios e regras decorrentes da legislação em matéria de proteção de dados pessoais, bem como ao controlo e fiscalização da Comissão Nacional de Proteção de Dados, no exercício das suas competências legais".

2. Políticas de proteção dos jogadores

Vamos então analisar seguidamente dois casos concretos em matéria de aplicação de políticas de proteção dos jogadores e processamento e tratamento dos seus dados pessoais, um em que a entidade exploradora é uma casa de apostas *online* e outro em que a entidade exploradora é um casino *online*. A casa de apostas online eleita é a **bet.pt**, acessível através do *link* <https://www.bet.pt/>, e o casino online o **888.pt**, acessível através do link <https://www.888.pt/>.

Começando por aquele que é, desde logo, o primeiro passo, necessário para utilizar este tipo de serviços: o registo da conta de utilizador. Dispõe o Art.º 37.º, n.º 1 do Decreto-Lei 66/2015 que "as entidades exploradoras são obrigadas a que o registo dos jogadores contenha: Nome completo, data de nascimento, nacionalidade, profissão, morada de residência, número de identificação civil, NIF, email e identificadores da conta de pagamento."

Acedendo à opção de registo no *site* da **bet.pt** <https://www.bet.pt/>, verificamos que numa primeira instância os dados pessoais solicitados são o género, o primeiro nome, os apelidos, a data de nascimento e o *email*.

Já o **888.pt**, começa por solicitar nome completo, país, email, data de nascimento e sexo, solicitando também desde logo que o utilizador marque uma checkbox, declarando que é maior de idade e que aceita os "Termos e Condições e a Política de Privacidade", aspetos que irão também ser abordados mais adiante. Para uma melhor perceção, além da descrição, são também ilustrados os passos necessários para efetivar o registo nestas entidades.

Figura 1 – Primeiro passo do registo nas entidades **bet.pt** (esquerda) e **888.pt** (direita).

Prosseguindo com o registo, o passo seguinte do **bet.pt** passa por solicitar ao jogador/cliente que insira o país, o número de telemóvel, a nacionalidade, a profissão, o NIF, o Número de Identificação Fiscal, o código postal, a morada e a cidade. Temos então que ficam apenas a faltar os dados identificadores da conta de pagamento e é pedido adicionalmente o número de telemóvel, relativamente ao que é exigido pelo Art.º 37.º, n.º 1.

No caso do **888.pt**, solicita um nome de utilizador, uma palavra-passe, uma pergunta e resposta de segurança para recuperação da password em caso de esquecimento, o NIF e o IBAN.

Figura 2 – Segundo passo do registo nas entidades bet.pt (esquerda) e 888.pt (direita).

Passamos então para o terceiro e último passo para a criação da conta no **bet.pt** que é a definição de um nome de utilizador, uma palavra-passe, e a especificação do IBAN da conta de pagamento, sendo então este o último dado que faltava inserir relativamente ao exigido por lei. De realçar a existência de um sistema "captcha", que tradicionalmente consiste num pequeno desafio cognitivo para garantir que é de facto um humano que se está a registar, e não um robô programado para efetuar registos em massa de forma automatizada. De notar também a existência da *checkbox* que o jogador deverá marcar, declarando que é maior de idade e que aceita os "Termos e Condições, Política de Privacidade, Regras de Apostas e Jogo Responsável", a qual no caso do **888.pt** foi apresentada logo no primeiro passo.

Relativamente ao último passo para efetivar o registo no **888.pt**, é solicitado ao jogador o código postal, a cidade, o endereço (morada), o número de telemóvel (opcional), a profissão, a nacionalidade e o número de identificação civil.

Figura 3 – Terceiro passo do registo nas entidades bet.pt (esquerda) e 888.pt (direita).

Temos então que em ambos os casos são solicitados aos utilizadores os dados exigidos na lei relativamente ao registo dos jogadores e especificado no Art.º 37º, n.º 1 do Decreto-Lei 66/2015. A identidade dos jogadores deverá depois ser verificada através de consulta às bases de dados de entidade pública, efetuada, em tempo real, através de ligação à entidade de controlo, inspeção e regulação, ou então diretamente no respetivo sítio na Internet, através de cartão do cidadão ou chave móvel digital, em consonância

com o n.º 2 do Art.º 37.º. De acordo com o n.º 3 do mesmo artigo, caso tal não seja possível, a verificação da identidade dos jogadores deverá ser efetuada através de cópia de documento comprovativo da identidade, com fotografia e data de nascimento. Diz-nos o n.º 5 que o registo de jogador só se torna efetivo depois de verificada a respetiva identidade e confirmada a inexistência de proibição de jogar.

A este respeito, é imprescindível a referência ao nº 7 do Art.º 47º do Decreto-Lei 66/2015, onde é disposto que: "Em respeito pelas regras de proteção dos dados pessoais, a entidade de controlo, inspeção e regulação cria e mantém atualizado um sistema de registo nacional centralizado dos jogadores que, voluntária ou judicialmente, estejam impedidos de jogar, o qual deve ser disponibilizado às entidades exploradoras."

Ainda a respeito da confirmação de identidade, ao consultar os Termos e Condições do site **bet.pt**, disponíveis em <https://www.bet.pt/politicas-jogo/termos-e-condicoes/>, no ponto 5.2 – Dados pessoais e verificação de identidade verifica-se que esta informação é efetivamente facultada tal como referido no nº 3 do Art.º 37.º. Já no *site* do **888.pt** não é mencionada a forma como será feita a verificação da identidade, sendo apenas referido no ponto 2 dos "Termos e Condições", acessíveis em <https://www.888.pt/seguranca-e-privacidade/acordo-do-utilizador/> que "Ao aceitar os presentes Termos e Condições autoriza-nos igualmente a confirmar e/ou verificar os seus dados pessoais, por forma a conferir a sua identidade, o que inclui, mas não se limita a, fornecer os seus dados pessoais a terceiros, nos termos permitidos por lei, para confirmar e/ou verificar os seus dados pessoais."

Supondo que um jogador, voluntária ou judicialmente, impedido de jogar com a sua identidade e os seus dados pessoais se registava novamente fornecendo dados falsos para poder continuar a jogar, tal seria punível ao abrigo do n.º 1 do Art.º 50.º da Lei 58/2019, de 8 de agosto: "Quem inserir ou facilitar a inserção de dados pessoais falsos, com a intenção de obter vantagem indevida para si ou para terceiro, ou para causar prejuízo, é punido com pena de prisão até 2 anos ou com pena de multa até 240 dias.". Tratar-se-ia de uma inserção de dados pessoais falsos para obter vantagem indevida que neste caso seria poder continuar a jogar, apesar da proibição.

A delimitação relativa às proibições de jogar, é especificada na lei através do Art.º 6.º do Decreto-Lei 66/2015, existindo mais uma vez nos "Termos e Condições" do *site* **bet.pt** uma transcrição do que é mencionado nesse artigo. Nos "Termos e Condições" do **888.pt**, no ponto 4 – Participação Permitida, também é feita essa mesma transcrição integral.

Importa referir que a lei obriga as entidades exploradoras a elaborar um plano e adotar medidas que garantam a prática de jogo responsável e proporcionem ao público, em especial aos jogadores, a necessária informação promovendo atitudes de jogo moderado, não compulsivo e responsável, conforme disposto no Art.º 7.º, nº 2. Este plano deverá incluir, de acordo com o n.º 3, b) "Política de informação e comunicação ao jogador sobre comportamentos responsáveis no jogo e os perigos da dependência e da adição ao jogo, que integre uma mensagem permanente sobre jogo responsável no sítio na Internet", e de acordo com o n.º 3 c) "Medidas adotadas pela entidade exploradora que visem proteger os menores, os incapazes e os que voluntariamente estejam impedidos de jogar e prevenir o acesso dos mesmos aos jogos e apostas online".

No **bet.pt**, em <https://www.bet.pt/politicas-jogo/jogo-responsavel/>, existe diversa informação a este respeito, nomeadamente um ponto onde são fornecidas dicas para autoavaliação de dependência e oferecidos alguns conselhos práticos, um que informa o jogador acerca de limites de jogo que este pode definir, um acerca da possibilidade de o jogador se autoexcluir por tempo por ele definido, e outro com contactos úteis para recorrer em caso de dependência. No **888.pt**, nomeadamente no link <https://www.888.pt/jogar-de-forma-responsavel/> também é fornecida diversa informação acerca de jogo compulsivo, meios para a sua prevenção, estabelecimento de autolimites de jogo, direito de autoexclusão, e fornecidos contactos para ajuda em caso de dependência. Quanto à apresentação de uma mensagem permanente sobre jogo responsável no sítio da Internet, tal sucede em ambos os casos, tal como ilustrado em seguida.

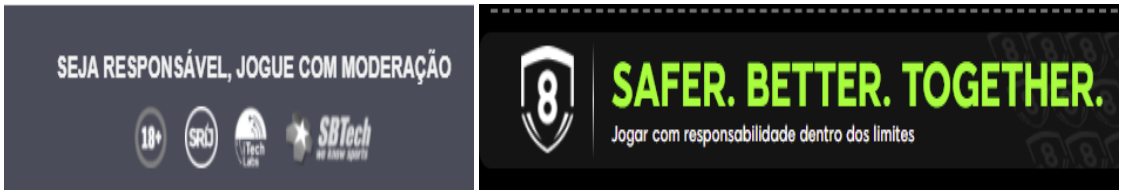


Figura 4 – Mensagem sobre jogo responsável do bet.pt (à esquerda) e 888.pt (à direita)

De acordo com o Art.º 30.º - Informação aos jogadores, deve ser facultada ao jogador toda a informação referente aos elementos acima mencionados, o que de facto se verifica. Dispõe também a alínea b) que deve ser facultada aos jogadores informação acerca do modo de acesso aos seus dados pessoais. Vamos então analisar se isso de facto acontece, começando pelo **bet.pt**.

Nos "Termos e Condições" do **bet.pt**, verificamos no número 11 a existência de informação relativa à política de privacidade, onde é mencionado que os dados de utilizador são considerados confidenciais e guardados em segurança de acordo com a "Política de Privacidade" da Gobet (entidade exploradora responsável pela gestão da plataforma digital **bet.pt**). Consta ainda que "Nos termos do regulamentado, o cliente fica sujeito ao cumprimento dos princípios e regras aplicáveis em matéria de proteção de dados pessoais, bem como ao controlo e fiscalização da Comissão Nacional de Proteção de Dados, enquanto autoridade de controlo nesta matéria.".

Em seguida, é disponibilizado um link para consulta de toda a política de privacidade, <https://www.bet.pt/politicas-jogo/privacidade/> no qual o ponto 2 faz referência ao tratamento de dados pessoais. Começa por referir em 2.1 que, de acordo com o Decreto-Lei nº 66/2015, tem o dever de recolher os dados referentes ao utilizador que já abordámos anteriormente, sendo obrigatória a também referida verificação de identidade. Em 2.2 é abordada a questão do sistema de consentimento, sendo informado que, quando estejam em causa finalidades de tratamento que não advenham de exigências legais ou que não sejam necessárias para a execução de um contrato, bem como não estando em causa interesses vitais ou a prossecução de um interesse legítimo da Gobet, os dados pessoais apenas poderão ser utilizados com base no consentimento prestado pelo titular para cada uma das finalidades. Mais, é dito que no âmbito da sua atividade a Gobet poderá recorrer a terceiros para a prestação de determinados serviços, podendo implicar o acesso, por estas entidades, a dados pessoais dos seus clientes/jogadores, e que assim sendo, o cliente/jogador terá de ser informado da(s) finalidade(s) para as quais a Gobet pretende tratar os seus dados e obter o seu consentimento para esse efeito. Assim, por forma a permitir que a Gobet o contacte por via de e-mail e/ou SMS para o contacto de telemóvel recolhido para o envio da sua newsletter e de promoções especiais, o cliente/jogador terá de prestar o seu consentimento expresso e informado.

Esta informação vai portanto de encontro aos princípios relativos ao tratamento de dados pessoais estipulados pelo Art.º 5.º do RGPD, aplicando-se também o disposto no Art.º 6º do mesmo regulamento, nomeadamente no nº 1: "O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: […] "b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;", dizendo esta parte respeito ao registo no *site* e à intenção do cliente/jogador em usufruir dos serviços, e "a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados

pessoais para uma ou mais finalidades específicas;", esta alínea relativa à eventual prestação de serviços por parte de terceiros a que a Gobet tenha de recorrer e que tenham acesso aos dados pessoais. As condições aplicáveis ao consentimento, estipuladas pelo Art.º 7.º estão em conformidade, sendo também referido que o cliente/jogador poderá retirar o consentimento que tenha prestado para o tratamento dos seus dados a qualquer momento, deixando estes de ser tratados se não existir um fundamento jurídico que exija o tratamento, indo de encontro ao disposto no nº 3 do mesmo artigo.

Ainda na política de privacidade do **bet.pt**, no ponto 2.3, é referido que, na prossecução de objetivos de prevenção e controlo da fraude e Branqueamento de Capitais e Financiamento do Terrorismo, a Gobet tem um interesse legítimo para as atividades de tratamento dos dados pessoais dos clientes/jogadores com essas finalidades. Esta situação também está prevista no RGPD, constando do Considerando (47) que "Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável."

O ponto 2.4 faz referência a dados pessoais sensíveis e alerta que a informação referente a clientes/jogadores em situação de autoexclusão poderá ser considerada, em alguns dos casos, como um dado relativo à saúde do cliente/jogador. Temos aqui patente a questão dos jogadores compulsivos, cuja condição pode ser considerada uma doença do foro psicológico e logo enquadrável no âmbito das categorias especiais de dados pessoais, regulamentada pelo Art.º 9.º do RGPD, nomeadamente "g) […] prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;" (trata-se aqui de um tratamento que visa salvaguardar os direitos e interesses do titular dos dados, tratando-se este de um jogador compulsivo, pelo que será um tratamento lícito) e "h) Se o tratamento for necessário para efeitos de […] prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros.". Esta alínea prevê e permite o tratamento de dados pessoais em matéria de dados de saúde, e vai de encontro ao que é enunciado pela política de privacidade do portal **bet.pt**.

Informa ainda este portal que o tratamento da informação dos clientes/jogadores em situação de autoexclusão não carece de consentimento dos titulares para a finalidade de o retirar e operacionalizar o impedimento de utilização da plataforma de jogo insere-

se no âmbito do cumprimento de uma obrigação legal definida no Decreto-Lei n.º 66/2015. Com efeito, o Art.º 39.º do Decreto-Lei obriga a entidade exploradora a disponibilizar no seu sítio da internet mecanismos que permitam ao jogador autoexcluir-se da prática de jogos e apostas *online*, sendo dever da entidade exploradora transmitir à entidade de controlo, inspeção e regulação a identificação dos jogadores que se autoexcluíram, no prazo máximo de 24 horas a contar da data da receção da respetiva comunicação, ao abrigo do Art.º 26.º p) do mesmo Decreto-Lei. A não disponibilização no sítio da Internet de mecanismos que permitam a autoexclusão dos jogadores constitui ao abrigo do Art.º 57.º n), uma contraordenação grave, e a não transmissão à entidade de controlo, inspeção e regulação da identificação dos jogadores que se autoexcluíram no prazo de 24 horas, é tida como uma contraordenação leve, punível ao abrigo do Art.º 58.º e).

Relativamente aos direitos dos titulares, o **bet.pt** informa que lhes é garantido o direito de informação no momento da recolha dos dados pessoais, relativamente aos contactos do responsável pelo tratamento, das finalidades do tratamento, do tempo limite de conservação, dos seus direitos enquanto titular dos dados, e da possibilidade de apresentação de queixa à autoridade de controlo e da eventual existência de decisões automatizadas e/ou definição de perfis. Constata-se que é cumprido o disposto no Art.º 13.º do RGPD, em matéria de informações a facultar quando os dados são recolhidos junto do titular. É ainda garantido ao titular o direito de acesso, podendo este obter a confirmação da existência ou não do tratamento dos seus dados pessoais, perguntar como obter acesso aos seus dados e obter uma cópia dos mesmos, de preferência em formato exportável, cruzando-se aqui com o direito à portabilidade, podendo o titular solicitar os dados pessoais num formato de uso frequente ou comum, por forma a operar a transferência para outra organização, mesmo que concorrente. O direito de acesso está previsto no Art.º 15.º do RGPD, sendo o direito à portabilidade contemplado no Art.º 20.º.

Informa ainda o **bet.pt** que o titular tem o direito de, a qualquer momento, corrigir, apagar ou bloquear o tratamento dos seus dados pessoais, estando cada uma destas situações previstas no RGPD nos Art.ºs 16.º, 17.º e 18.º, respetivamente.

Por fim, é ainda garantido ao titular o direito à limitação, isto é, a contestação da exatidão dos dados pessoais durante um período que permita ao responsável pelo tratamento verificar a sua exatidão, previsto pelo já referido Art.º 18.º do RGPD, e o direito à remoção/esquecimento, em que o titular pode solicitar a remoção dos seus dados

e a eliminação definitiva dos que não colidam com obrigações legais, conforme o também já mencionado Art.º 17.º do RGPD.

Passemos então para a informação facultada pelo **888.pt** em termos de acesso e tratamento de dados pessoais. Nos "Termos e Condições", é de imediato exposto que o utilizador ao aceitar os mesmos está a autorizar a entidade exploradora a confirmar e verificar os seus dados pessoais, por forma a conferir a sua identidade, o que inclui, mas não se limita a, fornecer os seus dados pessoais a terceiros, nos termos permitidos por lei, para confirmar e/ou verificar os seus dados pessoais. São depois enumerados na "Política de Privacidade", acessível em <https://www.888.pt/seguranca-e-privacidade/politica-de-privacidade/>, os elementos que o jogador deverá facultar sobre si, os quais já foram abordados anteriormente. Salvaguarda depois a eventual necessidade de "fornecer uma cópia de um ID emitido pelo governo para o processo de verificação da identidade", não sendo tal um requisito para a utilização de todos os recursos. Curioso é o facto de ser mencionada a recolha de padrões de jogo por forma a identificar possíveis problemas de vícios de jogo, garantindo assim o cumprimento das políticas de jogo responsável. O titular é também informado de que serão recolhidas informações acerca do seu dispositivo, tais como IMEI, MAC, endereço IP e dados de geolocalização. A propósito desta questão, será interessante referir que o RGPD tem em consideração a possibilidade de associação desta informação a pessoas singulares, quando refere no Considerando (30) que "as pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares." Partindo deste pressuposto, poderá ser considerada a hipótese de, quando combinados com outras informações, estes elementos poderem também ser considerados dados pessoais.

Relativamente ao processamento de dados pessoais, refere o **888.pt** que poderá fazê-lo no âmbito do contrato de utilizador, ou para cumprir as diversas responsabilidades legais e/ou regulamentares e cumprir legislação AML (*Anti-Money Laundering* – Anti lavagem de dinheiro) e KYC (*Know Your Customer* – Conhecer o cliente). Nestes casos, o tratamento será lícito, cumprindo o disposto no Art.º 6.º do RGPD. Quanto ao consentimento, é mencionado que o processamento das informações pessoais será

principalmente necessário para o fornecimento dos serviços, podendo em outras situações ser solicitado o consentimento para processar as informações pessoais. Nesse caso, as informações serão processadas de acordo com esse consentimento, o qual poderá ser retirado por escrito a qualquer momento. Cumprem-se assim as condições aplicáveis ao consentimento previstas no Art.º 7.º do RGPD. Há também referência às categorias especiais de dados pessoais, salvaguardando-se que estes possam ser processados e divulgados a autoridades competentes para fins tais como prevenção ou deteção de um ato ilegal, prevenção de condutas impróprias ou salvaguarda de bem-estar económico, ou retenção de informações referentes a questões de jogo responsável, indo de encontro ao estipulado no Art.º 9.º do RGPD e deixando também explícita a possibilidade e licitude do tratamento de dados relativos a jogadores compulsivos, contemplada em g) e h).

É feita a chamada de atenção segundo a qual os menores de 18 anos não deverão utilizar os serviços nem fornecer informações pessoais, reservando-se a entidade exploradora o direito de aceder e confirmar quaisquer informações pessoais, o que vai de encontro às políticas de proteção de menores e pessoas vulneráveis estipulada pelo Art.º 7.º n.º 3 c) do Decreto-Lei 66/2015 e da proibição de jogo a menores estipulada pelo Art.º 6.º d), do mesmo Decreto-Lei. É também apresentada na política de privacidade uma extensa lista com as finalidades para as quais são utilizadas as informações pessoais, nomeadamente para efeitos de criação de conta, disponibilização de serviços, elaboração de análises e estatísticas, garantia de ambiente de jogo responsável, detetar atividade fraudulenta e ilegal. Já vimos anteriormente, no caso do **bet.pt**, que o tratamento de dados para efeitos de disponibilização de serviço, prevenção de atividade fraudulenta e proteção de menores e pessoas vulneráveis é lícita. Acresce aqui a questão da elaboração de análises e estatísticas, que também está prevista no RGPD através do Art.º 5.º n.º 1 b), o qual dispõe que: "[o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («limitação das finalidades»);"

Existe ainda no **888.pt** a chamada de atenção quanto às informações pessoais irem ser utilizadas pelos próprios ou por terceiras entidades para efeitos relacionados com marketing, podendo este tipo de ofertas ser recusadas a qualquer momento, e sendo fornecidas as instruções para tal. É também referido que as informações pessoais poderão ser partilhadas com destinatários, tais como prestadores de serviços para operar a plataforma, empresas do grupo e outras afiliadas, agências de referência de crédito (as

quais irão depois com base nessa informação fornecer à entidade exploradora um cadastro financeiro do jogador), prestadores de serviços de pagamento, auditores, órgãos relacionados com o vício em jogos de aposta, entre outros. Cumpre-se também aqui o estipulado no Art.º 6.º do RGPD relativamente à licitude do tratamento.

Relativamente aos direitos dos titulares, o **888.pt** informa que qualquer contacto deverá ser efetuado via e-mail e poderá ser solicitado: "O acesso, alteração ou eliminação de dados pessoais; A restrição da utilização das informações pessoais; A disponibilização dos dados pessoais num formato legível por máquina; O retirar do consentimento relativamente a atividades de processamento que sejam baseadas no consentimento e não numa base legal diferente". Cumpre-se aqui o estipulado pelos Art.ºs 15.º, 16.º, 17.º e 18.º do RGPD em matéria de acesso, retificação, apagamento e limitação do tratamento dos dados, subentendendo-se o direito à portabilidade quando é mencionada a exportação dos dados num formato legível por máquina, previsto pelo Art.º 20º.

Relativamente à disponibilização de mecanismos de autoexclusão, tal como já havia sido referido anteriormente, existe nos "Termos e Condições" do **888.pt** um link direto para a política de jogo responsável, acessível em https://www.888.pt/jogar-de-forma-responsavel/> ,onde são dadas algumas dicas quer para prevenção do jogo por parte de menores, quer para prevenção do jogo compulsivo, indicando a possibilidade de obter aconselhamento e ajuda através do "Serviço Linha Vida", de impor limites aos valores a apostar, bem como o de se autoexcluir por um período de 3 meses, ou mais prolongado, remetendo neste caso para o preenchimento de um formulário no site do Serviço de Inspeção e Regulação de Jogos que fará com que o jogador fique impedido de jogar e apostar nos sites de todas as entidades exploradoras. O disposto no Art.º 39.º do Decreto-Lei 66/2015 é assim cumprido com a disponibilização de mecanismos de autoexclusão.

3. Considerações finais

Verifica-se então que, embora organizando e disponibilizando a informação de formas distintas, quer a casa de apostas **bet.pt**, quer o casino *onlin*e 888.**pt** cumprem as suas obrigações legais em matéria de aplicação de políticas de proteção dos jogadores e processamento e tratamento de dados pessoais dos mesmos. De resto, outra coisa não seria expectável atendendo a que estas entidades, bem como as restantes pertencentes ao mesmo sector são rigidamente reguladas pelo Serviço de Regulação e Inspeção de Jogos

do Turismo de Portugal, devendo seguir à risca todas as normas e diretrizes da legislação portuguesa no que toca a jogo online.

4. Referências documentais:

Decreto-Lei nº 66/2015, de 29 de abril, acessível em: <https://dre.pt/web/guest/pesquisa/-/search/67098359/details/maximized>;

Regulamento(UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), acessível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>;

Lei n.º 58/2019, de 8 de agosto, acessível em: <https://dre.pt/pesquisa/-/search/123815982/details/maximized>;

Página oficial da casa de apostas desportivas **bet.pt**, acessível em: <https://www.bet.pt/>;
"Termos e Condições" da casa de apostas desportivas **bet.pt**, acessível em: <https://www.bet.pt/politicas-jogo/termos-e-condicoes/>;
"Política de jogo responsável" da casa de apostas desportivas **bet.pt**, acessível em: <https://www.bet.pt/politicas-jogo/jogo-responsavel/>;
"Política de privacidade" da casa de apostas desportivas **bet.pt**, acessível em: <https://www.bet.pt/politicas-jogo/privacidade/>;
Página oficial do casino *online* **888.pt**, acessível em: <https://casino.888.pt/>;
"Termos e Condições" do casino *online* **888.pt**, acessível em: < https://www.888.pt/seguranca-e-privacidade/acordo-do-utilizador/>;
"Política de jogo responsável" do casino *online* **888.pt**, acessível em: <https://www.888.pt/jogar-de-forma-responsavel/>;
"Política de privacidade" do casino *online* **888.pt**, acessível em: <https://www.888.pt/seguranca-e-privacidade/politica-de-privacidade/>.

III_Legislação e Jurisprudência Comentadas

Regulamento Inteligência Artificial

Artificial Intelligence Act

Cristina Maria de Gouveia Caldeira[297]

Introdução Geral

Em 21 de abril de 2021, a Comissão Europeia apresentou uma Proposta de Regulamento do Parlamento Europeu e do Conselho, relativa ao estabelecimento de regras harmonizadas sobre a inteligência artificial (Regulamento Inteligência Artificial/*Artificial Intelligence Act*)[298], colocando-se na vanguarda dos sistemas de inteligência artificial (IA).

Na referida proposta, estabelece-se um quadro jurídico aplicável aos sistemas de IA[299], no qual se prevê regras e novas obrigações, num âmbito de aplicação alargado, que se estende à maioria dos intervenientes na cadeia de produção de IA (fornecedores de IA, entidades que utilizam sistemas de IA, importadores, distribuidores, fabricantes de produto e representantes autorizados[300]. Relativamente ao seu âmbito territorial, o mesmo será aplicável às entidades, mesmo que não se encontrem estabelecidas na União Europeia, sendo apenas necessário que o sistema de IA seja colocado no mercado ou ao

[297] Pós-Doutorada na área da Propriedade Intelectual, Universidade Nova de Lisboa e investigadora de pós-doutoramento na Pontifícia Universidade Católica (PUCRS), Brasil. Doutorada em Direito na Especialidade em Ciências Jurídicas e Políticas pela Universidade Autónoma de Lisboa (UAL) e Programa Doutoral em Ciência Política na especialidade de políticas públicas, Universidade Católica Portuguesa. Bolseira da Fundação Gulbenkian na Universidade de Oxford, St Antony's College. Colabora no Laboratório de Bioética no Hospital de Clínicas (RS Brasil), como investigadora na área de proteção de Tecnologia e Ensino Superior. Coautora de projetos de diplomas legais. Foi Vice-Reitora do IADE-U – Instituto de Arte, Design e Empresa – Universitário (2014-2015). É Diretora Executiva da Revista Privacy and Data Protection Magazine e Cocoordenadora Privacy and Data Protection Centre. Autora de várias publicações e participante regular em iniciativas públicas de Direito da Propriedade Intelectual e Proteção de Dados. Encarregada de Proteção de Dados do Município de Lisboa (2021). Curriculum vitae: Ciência ID: 711B-87B9-6826. ORCID ID: https://orcid.org/0000-0001-6925-1877.

[298] COMISSÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União, COM(2021)206 final, Bruxelas, 21 de abril de 2021.
https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[299] O n.º 1 do artigo 3.º da Proposta de Regulamento Inteligência artificial define «Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage;».

[300] *Idem*, alínea *a*) do n.º 1 do artigo 2.º.

serviço do mercado europeu, ou ainda que o resultado produzido pelo sistema de IA seja utilizado na União Europeia[301].

O diploma vai além da componente legal, ao reforçar a componente ética, indo ao encontro do *Regime relativo aos aspetos éticos da Inteligência Artificial, da robótica e das tecnologias conexas*, apresentado pelo Parlamento Europeu, numa Resolução que integra uma parte da proposta legislativa de um regulamento relativo aos princípios éticos para o desenvolvimento da IA, da robótica e das tecnologias conexas, de 20 de outubro de 2020[302]. O diploma agora proposto traduz um compromisso político assumido pela presidente Usula von der Leyen, que tem a legitima ambição de alcançar a liderança global em matéria de IA, maximizando os seus benefícios, ao mesmo tempo que coloca o ser humano no centro de um ecossistema sustentável, seguro, inclusivo e confiável.

O diploma prevê os seguintes objetivos específicos[303]:

- garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União,
- garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA,
- melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA,
- facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado.

O quadro regulamentar sobre IA é baseado no risco e diferencia entre as utilizações que criam: i) um risco inaceitável, ii) um risco elevado e iii) um risco baixo ou mínimo. O título II do diploma estabelece a proibição de determinadas práticas de inteligência artificial[304], por considerar que conflituam com os valores da União Europeia, por exemplo por violar os direitos fundamentais, e dessa forma traduz um risco inaceitável.

Da lista de práticas de IA proibidas constantes do título II, constam os sistemas de inteligência artificial que utilizem técnicas de manipulação do subconsciente ou explorem vulnerabilidades de grupos especialmente frágeis como crianças, pessoas com deficiência, por forma a distorcer materialmente o seu comportamento provocando-lhe

[301] *Idem*, alínea *c)* do n.º 1 do artigo 2.º.
[302] PARLAMENTO EUROPEU. Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas (2020/2012(INL). https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.html#title1.
[303] COMISSÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. COM(2021) 206 final. Bruxelas, 21.04.2021, p. 3.
[304] *Idem*, artigo 5.º.

um dano físico ou psicológico à pessoa ou a um terceiro. O diploma refere ainda como risco inaceitável, a utilização em espaços públicos de sistemas de identificação biométrica à distância em tempo real para efeitos policiais, excetuando certos casos específicos como a busca por crianças desaparecidas ou a prevenção de um ataque terrorista (ainda assim mediante autorização prévia por parte de uma autoridade judicial ou administrativa independente).

Mas a Proposta de Regulamento vai mais longe ao considerar no Título III, que certos sistemas de inteligência artificial são dotados de um risco elevado para a saúde, segurança e direitos fundamentais das pessoas, designadamente os sistemas utilizados na gestão do tráfego rodoviário, no recrutamento ou seleção de pessoas, entre outros[305]. Nestes casos são previstos requisitos apertados dirigidos a estes sistemas de IA, impondo-se a necessidade de implementação de um sistema de gestão do risco[306], de cumprimento de requisitos relativos à qualidade dos dados utilizados, disponibilidade de documentação técnica e conservação de registos, prestação de informação aos utilizadores, supervisão humana e requisitos de segurança dos sistemas. São também estabelecidos requisitos dirigidos especificamente aos sujeitos que operam com esses sistemas[307].

Para assegurar a coerência, evitar as duplicações e minimizar os encargos adicionais, os sistemas de IA de risco elevado presentes nesta proposta, serão integrados na legislação de segurança setorial em vigor. Com particular destaque para os sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação do novo quadro legislativo (NQL), a exemplo de máquinas, dispositivos médicos e brinquedos[308].

A proposta acompanha a estratégia digital global da Comissão no contributo que presta para promover o conceito de «tecnologia ao serviço das pessoas», um dos três principais pilares da orientação política e dos objetivos anunciados na Comunicação «Construir o futuro digital da Europa». Está igualmente associada à Proposta de regulamento relativo à governação de dados [COM(2021)767] e a outras iniciativas estabelecidas pela União Europeia nessa matéria[309].

[305] *Idem*, Anexo III *ex vi* do artigo 6.º.
[306] Para as instituições de crédito sujeitas à Diretiva 2013/36/UE, o referido sistema de gestão de risco deverá ser integrado nos procedimentos de gestão de risco estabelecidos nos termos do artigo 74.º da referida diretiva (artigo 9.º, n.º 9 da Proposta de Regulamento).
[307] Cfr. COMISSÃO EUROPEIA. Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União. COM(2021) 206 final. Bruxelas, 21.04.2021, artigos 16.º a 29.º.
[308] *Idem*, p. 4.
[309] *Idem*, p. 6.

A proposta completa ainda o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679] e a Diretiva sobre a Proteção de Dados na Aplicação da Lei [Diretiva (UE) 2016/680], ao mesmo tempo que garante a coerência com a Carta dos Direitos Fundamentais da UE e a legislação derivada da União em vigor em matéria de proteção de dados, defesa dos consumidores, não discriminação e igualdade de género[310].

Um outro aspeto relevante consiste nas obrigações de transparência previstas no Título IV e que recai sobre os sistemas que *(i)* interagem com humanos, ou *(ii)* são utilizados para detetar emoções, ou *(iii)* geram ou manipulam conteúdos (*deep fakes*). Nestas situações as pessoas devem ser informadas que estão a interagir com sistemas de inteligência artificial, que as suas emoções são reconhecidas por um sistema ou ainda que o sistema é utilizado para manipular o conteúdo de uma imagem, áudio ou vídeo, por forma a realizarem as suas escolhas de maneira informada.

Os fornecedores de sistemas de inteligência artificial classificados de baixo risco**,** poderão aderir voluntariamente ao cumprimento dos requisitos estabelecidos na Proposta de Regulamento através da criação e implementação dos seus próprios códigos de conduta, podendo incluir compromissos voluntários de sustentabilidade ambiental, tal como se prevê no Título IX.

Face ao incumprimento das obrigações previstas no diploma, a Proposta de Regulamento estabelece um regime sancionatório exigente com um teto máximo de 30.000 ou, no caso de empresas e consoante o que for mais elevado, até 6% do volume de negócios total anual, à escala mundial, relativo ao exercício financeiro anterior.

A Proposta de regulamento prevê um sistema de governação no Título VI, que se baseia na criação de um Comité Europeu para a Inteligência Artificial a nível da União e, de autoridades nacionais de controlo, para efeitos de supervisão da aplicação e da execução do regulamento, ao nível nacional. No âmbito do presente regulamento, as instituições, órgãos e organismos da União serão supervisionados pela Autoridade Europeia para a Proteção de Dados.

A Proposta de Regulamento será ainda submetida ao processo legislativo ordinário, mas não restam dúvidas que coloca a União Europeia na vanguarda a nível mundial no que concerne à regulação no domínio da inteligência artificial, centrada na dignidade do ser humano, o que lhe permite oferecer as garantias de proteção dos direitos fundamentais e da segurança dos cidadãos, ao mesmo tempo que impulsiona a investigação e a inovação e promove a competitividade e a capacidade industrial.

[310] *Idem Ibidem*.

COMISSÃO
EUROPEIA

Bruxelas, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

Exposição de Motivos

1.CONTEXTO DA PROPOSTA
1.1. Razões e objetivos da proposta

A presente exposição de motivos acompanha a proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial). A inteligência artificial (IA) é uma família de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente e conceder vantagens competitivas às empresas e à economia europeia. Essa ação torna-se especialmente necessária em setores de elevado impacto, incluindo os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura. Contudo, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem trazer novos riscos ou consequências negativas para os cidadãos e a sociedade. À luz da velocidade da evolução tecnológica e dos possíveis desafios, a UE está empenhada em alcançar uma abordagem equilibrada. É do interesse da União preservar a liderança tecnológica da UE e assegurar que novas tecnologias, desenvolvidas e exploradas respeitando os valores, os direitos fundamentais e os princípios da União, estejam ao serviço dos cidadãos europeus.

A presente proposta honra o compromisso político assumido pela presidente Ursula von der Leyen, que anunciou nas suas orientações políticas para 2019-2024, intituladas «Uma União mais ambiciosa»1, que a Comissão apresentaria uma proposta legislativa relativa a uma abordagem europeia coordenada às implicações humanas e éticas da inteligência artificial. Na sequência desse anúncio, a Comissão publicou, em 19 de fevereiro de 2020, o Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança 2. O Livro Branco define as opções políticas sobre a forma de alcançar o duplo objetivo de promover a adoção da IA e de abordar os riscos associados a determinadas utilizações desta tecnologia. A presente proposta visa dar execução ao segundo objetivo, desenvolvendo um ecossistema de confiança mediante a proposta de um quadro jurídico para uma IA de confiança. A proposta tem como base os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a confiança necessária para adotarem soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos. As regras aplicáveis às tecnologias de inteligência artificial disponibilizadas no mercado da União ou que afetam as pessoas da União devem, por isso, centrar-se no ser humano, de modo que as pessoas possam confiar que a tecnologia é utilizada de uma forma segura e em cumprimento da lei, incluindo em matéria de respeito dos direitos fundamentais. Na sequência da publicação do Livro Branco, a Comissão lançou uma consulta abrangente das partes interessadas, a qual revelou um grande interesse por parte de um vasto número de partes que apoiaram amplamente a intervenção regulamentar com vista a resolver os desafios e as preocupações relacionadas com a crescente utilização da IA.

A proposta também dá resposta a pedidos explícitos do Parlamento Europeu e do Conselho Europeu, que têm apelado, repetidamente, para a ação legislativa, com vista a assegurar o bom funcionamento do mercado interno de sistemas de inteligência artificial («sistemas de IA»), no qual os benefícios e os riscos da IA sejam abordados de forma adequada a nível da União. A proposta apoia o objetivo da União de estar na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança, conforme mencionado pelo Conselho Europeu3 , e garanta a proteção de princípios éticos, conforme pedido especificamente pelo Parlamento Europeu4 .

Em 2017, o Conselho Europeu apelou para que fosse tomada a «consciência da urgência em fazer face às tendências emergentes, entre as quais se contam a inteligência artificial [...], com a garantia simultânea de um elevado nível de proteção dos dados, direitos digitais e normas éticas» 5 . Nas suas Conclusões sobre o plano coordenado para o desenvolvimento e utilização da inteligência artificial «Made in Europe», de 2019 6 , o Conselho continuou a destacar a importância de assegurar o pleno respeito dos direitos dos cidadãos europeus e apelou para uma reapreciação da legislação pertinente em vigor, para torná-la adequada à sua finalidade no que respeita às novas oportunidades que a inteligência artificial oferece e aos desafios que coloca. O Conselho Europeu também convidou a Comissão a definir claramente as aplicações de inteligência artificial que devem ser consideradas de risco elevado.

As Conclusões, mais recentes, de 21 de outubro de 2020 reforçaram a importância de dar resposta a desafios como a opacidade, a complexidade, os preconceitos [ou enviesamentos], um certo grau de imprevisibilidade e comportamentos parcialmente autónomos de determinados sistemas de IA, a fim de garantir a compatibilidade destes sistemas com os direitos fundamentais e facilitar a aplicação das normas jurídicas.

O Parlamento Europeu também realizou um trabalho considerável no domínio da IA. Em outubro de 2020, adotou um conjunto de resoluções no domínio da IA, nomeadamente em matéria de ética 9 , responsabilidade 10 e direitos de autor 11 . Em 2021, seguiram-se resoluções no domínio da IA em matéria penal 12 e nos domínios da educação, da cultura e do setor audiovisual 13 . A Resolução do Parlamento Europeu sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas recomenda especificamente à Comissão que proponha uma ação legislativa para tirar partido dos benefícios e das oportunidades da IA, mas também para garantir a proteção de princípios éticos. A resolução inclui uma parte da proposta legislativa de um regulamento relativo aos princípios éticos para o desenvolvimento, implantação e utilização da inteligência artificial, da robótica e das tecnologias conexas. Em conformidade com o compromisso político assumido pela presidente Ursula von der Leyen nas suas orientações políticas relativamente às resoluções adotadas pelo Parlamento Europeu nos termos do artigo 225.º do TFUE, a presente proposta tem em conta a resolução acima mencionada do Parlamento Europeu, no pleno respeito dos princípios da proporcionalidade, da subsidiariedade e da iniciativa Legislar Melhor.

Tendo em conta este contexto político, a Comissão apresenta uma proposta de quadro regulamentar em matéria de inteligência artificial com os seguintes objetivos específicos:

- garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União,

- garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA,
- melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA,
- facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado.

Para alcançar esses objetivos, a presente proposta apresenta uma abordagem regulamentar horizontal equilibrada e proporcionada ao domínio da inteligência artificial, que se limita aos requisitos mínimos necessários para dar resposta aos riscos e aos problemas associados à IA, sem restringir ou prejudicar indevidamente a evolução tecnológica ou aumentar desproporcionalmente o custo de colocação no mercado das soluções de IA. A proposta estabelece um quadro jurídico sólido e flexível. Por um lado, as suas escolhas regulamentares fundamentais, incluindo os requisitos baseados em princípios que os sistemas de IA devem respeitar, são abrangentes e estão preparadas para o futuro. Por outro lado, cria um sistema regulamentar proporcionado, centrado numa abordagem regulamentar baseada no risco bem definida que não cria restrições desnecessárias ao comércio e na qual a intervenção jurídica é adaptada às situações concretas em que existe um motivo de preocupação justificado ou em que tal preocupação pode ser razoavelmente antecipada num futuro próximo. Ao mesmo tempo, o quadro jurídico inclui mecanismos flexíveis que permitem a sua adaptação dinâmica à medida que a tecnologia evolui e surgem novas situações preocupantes.

A proposta estabelece regras harmonizadas para o desenvolvimento, a colocação no mercado e a utilização de sistemas de IA na União na sequência de uma abordagem proporcionada baseada no risco. Propõe-se uma definição inequívoca e preparada para o futuro de «inteligência artificial». Algumas práticas de IA particularmente prejudiciais são proibidas, uma vez que violam os valores da União, e são propostas restrições e salvaguardas específicas relativamente a determinadas utilizações de sistemas de identificação biométrica à distância para efeitos de manutenção da ordem pública. A proposta estabelece uma metodologia de análise de riscos sólida para definir sistemas de IA de «risco elevado» que criam riscos significativos para a saúde e a segurança ou para os direitos fundamentais das pessoas. Esses sistemas de IA terão de cumprir um conjunto de requisitos obrigatórios horizontais para uma IA de confiança e seguir procedimentos de avaliação da conformidade antes de poderem ser colocados no mercado da União. Os fornecedores e os utilizadores desses sistemas também estão sujeitos a obrigações previsíveis, proporcionadas e claras para garantir a segurança e o respeito da legislação em vigor que protege os direitos fundamentais ao longo de todo o ciclo de vida dos sistemas de IA. No caso de alguns sistemas de IA específicos, apenas são propostas obrigações de transparência mínimas, em particular quando são utilizados sistemas de conversação automática ou «falsificações profundas».

As regras propostas serão executadas por intermédio de um sistema de governação a nível dos Estados-Membros, aproveitando estruturas já existentes, e de um mecanismo de cooperação a nível da União, ou seja, o novo Comité Europeu para a Inteligência Artificial. Também são propostas medidas adicionais para apoiar a inovação, em particular por via de ambientes de testagem da regulamentação da IA e de outras medidas que visam reduzir os encargos regulamentares e apoiar as pequenas e médias empresas (PME) e as empresas em fase de arranque.

1.2. Coerência com as disposições existentes da mesma política setorial

A natureza horizontal da proposta exige a plena coerência com a legislação da União em vigor aplicável aos setores em que os sistemas de IA de risco elevado já são utilizados ou serão provavelmente utilizados num futuro próximo.

É igualmente garantida coerência com a Carta dos Direitos Fundamentais da UE e a legislação derivada da União em vigor em matéria de proteção de dados, defesa dos consumidores, não discriminação e igualdade de género. A proposta não prejudica e completa o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679] e a Diretiva sobre a Proteção de Dados na Aplicação da Lei [Diretiva (UE) 2016/680] com um conjunto de regras harmonizadas aplicáveis à conceção, ao desenvolvimento e à utilização de determinados sistemas de IA de risco elevado e restrições a determinadas utilizações de sistemas de identificação biométrica à distância. Além disso, a proposta completa o direito da União em vigor em matéria de não discriminação com requisitos específicos que visam minimizar o risco de discriminação algorítmica, em particular no que diz respeito à conceção e à qualidade dos conjuntos de dados utilizados no desenvolvimento de sistemas de IA, complementados com obrigações de testagem, gestão de riscos, documentação e supervisão humana ao longo do ciclo de vida dos sistemas de IA. A proposta não prejudica a aplicação do direito da concorrência da União.

No que diz respeito aos sistemas de IA de risco elevado que são componentes de segurança de produtos, a presente proposta será integrada na legislação de segurança setorial em vigor para assegurar a coerência, evitar as duplicações e minimizar os encargos adicionais. Em particular, no que diz respeito aos sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação do novo quadro legislativo (NQL) (por exemplo, máquinas, dispositivos médicos, brinquedos), os requisitos aplicáveis aos sistemas de IA estabelecidos na presente proposta serão verificados no âmbito dos procedimentos de avaliação da conformidade previstos na correspondente legislação do NQL. No que diz respeito à interligação dos requisitos, embora os riscos de segurança específicos dos sistemas de IA devam ser abrangidos pelos requisitos da presente proposta, a legislação do NQL visa assegurar a segurança global do produto final e, como tal, pode incluir requisitos específicos relativos à integração segura de um sistema de IA no produto final. A proposta de regulamento relativo às máquinas, que é adotada no mesmo dia que a presente proposta, reflete plenamente esta abordagem. A presente proposta não é diretamente aplicável aos sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação da «antiga abordagem» (por exemplo, aviação, automóveis). Contudo, os requisitos essenciais ex ante aplicáveis aos sistemas de IA de risco elevado estabelecidos na presente proposta terão de ser tidos em conta aquando da adoção de atos de execução ou delegados ao abrigo dessa legislação.

No que diz respeito aos sistemas de IA fornecidos ou utilizados por instituições de crédito regulamentadas, as autoridades responsáveis pela supervisão da legislação da União em matéria de serviços financeiros devem ser designadas autoridades competentes para a supervisão dos requisitos estabelecidos na presente proposta, para assegurar uma execução coerente das obrigações previstas na presente proposta e da legislação da União em matéria de serviços financeiros nos casos em que os sistemas de IA sejam, até certo ponto, implicitamente regulamentados relativamente ao sistema de governação interno das instituições de crédito. A fim de aumentar a coerência, o procedimento de avaliação da conformidade e algumas das obrigações processuais dos fornecedores impostas nos termos da presente proposta são integradas nos procedimentos previstos na

Diretiva 2013/36/UE relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial 14 .

A presente proposta é coerente com o direito da União aplicável em matéria de serviços, incluindo os serviços intermediários regulamentados pela Diretiva 2000/31/CE (Diretiva sobre o comércio eletrónico) 15 e pela proposta de Regulamento Serviços Digitais (RSD) 16 recentemente apresentada pela Comissão.
Relativamente aos sistemas de IA que são componentes de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça geridos pela Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), a proposta não se aplica aos sistemas de IA que sejam colocados no mercado ou colocados em serviço antes de ter decorrido um ano desde a data de aplicação do presente regulamento, salvo se a substituição ou alteração desses atos jurídicos implicar uma alteração significativa da conceção ou da finalidade prevista do sistema ou dos sistemas de IA em causa.

1.3.Coerência com as outras políticas da União
A proposta faz parte de um pacote abrangente de medidas que visa resolver os problemas decorrentes do desenvolvimento e da utilização da IA, examinados no Livro Branco sobre a inteligência artificial. Como tal, é garantida a coerência e a complementaridade com outras iniciativas em curso ou planeadas da Comissão que também visam responder a esses problemas, incluindo a revisão da legislação setorial em matéria de produtos (por exemplo, a Diretiva Máquinas e a Diretiva Segurança Geral dos Produtos) e as iniciativas que abordam questões de responsabilidade associadas às novas tecnologias, incluindo os sistemas de IA. Essas iniciativas desenvolvem e completam a presente proposta, a fim de conferir certeza jurídica e promover o desenvolvimento de um ecossistema de confiança em matéria de IA na Europa.

A proposta é ainda coerente com a estratégia digital global da Comissão no contributo que presta para promover o conceito de «tecnologia ao serviço das pessoas», um dos três principais pilares da orientação política e dos objetivos anunciados na Comunicação «Construir o futuro digital da Europa» 17 . Estabelece um quadro coerente, eficaz e proporcionado para assegurar que a IA seja desenvolvida de modo que respeite os direitos das pessoas e conquiste a sua confiança, preparando a Europa para a era digital e transformando os próximos dez anos na Década Digital 18 .

Além disso, a promoção da inovação baseada na IA está estreitamente associada ao Regulamento Governação de Dados 19 , à Diretiva Dados Abertos 20 e a outras iniciativas estabelecidas na Estratégia europeia para os dados 21 , que criarão mecanismos e serviços de confiança para a reutilização, a partilha e o agrupamento de dados, elementos essenciais para o desenvolvimento de modelos de IA baseados em dados de elevada qualidade.

A proposta também reforça de forma significativa o papel da União na definição de regras e padrões mundiais e promove uma IA de confiança que é coerente com os valores e os interesses da União. Constitui uma base importante para a União continuar a colaborar com os parceiros externos, incluindo os países terceiros, e em fóruns internacionais em questões relacionadas com a IA.

2.BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

2.1.Base jurídica

A base jurídica da proposta é, em primeiro lugar, o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que prevê a adoção de medidas para assegurar o estabelecimento e o funcionamento do mercado interno.

A presente proposta constitui uma parte fundamental da estratégia para o mercado único digital da UE. O principal objetivo da presente proposta é assegurar o correto funcionamento do mercado interno mediante a criação de regras harmonizadas para o desenvolvimento, a colocação no mercado da União e a utilização de produtos e serviços que integram tecnologias de IA ou que são fornecidos como sistemas de IA autónomos. Alguns Estados-Membros já estão a ponderar regras nacionais para assegurar que a inteligência artificial seja segura e seja desenvolvida e utilizada em conformidade com as obrigações de proteção dos direitos fundamentais. Esta situação é suscetível de gerar dois grandes problemas: i) uma fragmentação do mercado interno no que diz respeito aos elementos essenciais relativos aos requisitos aplicáveis aos produtos e serviços baseados na inteligência artificial, à respetiva comercialização, utilização, responsabilidade e supervisão pelas autoridades públicas; ii) a redução substancial da segurança jurídica para os fornecedores e os utilizadores de sistemas de IA no que se refere à forma como as regras em vigor e as novas regras serão aplicadas a esses sistemas na União. Dada a vasta circulação de produtos e serviços entre fronteiras, a melhor solução para estes dois problemas passa por recorrer à legislação de harmonização da UE.

Efetivamente, a proposta define requisitos obrigatórios comuns aplicáveis à conceção e ao desenvolvimento de determinados sistemas de IA antes de estes serem colocados no mercado, os quais serão subsequentemente operacionalizados por via de normas técnicas harmonizadas. A proposta também aborda a situação após a colocação no mercado de sistemas de IA, por meio da harmonização do método de realização dos controlos ex post. Além disso, tendo em conta que a presente proposta contém determinadas regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, é adequado basear o presente regulamento no artigo 16.º do TFUE, no respeitante a essas regras específicas.

2.2.Subsidiariedade (no caso de competência não exclusiva)

A natureza da inteligência artificial, que muitas vezes depende de conjuntos de dados amplos e variados e pode ser integrada em qualquer produto ou serviço que circule livremente no mercado interno, implica que os objetivos da presente proposta não podem ser alcançados com eficácia apenas pela ação dos Estados-Membros. Além disso, a emergência de um mosaico de regras nacionais potencialmente divergentes prejudicaria a circulação homogénea de produtos e serviços associados a sistemas de IA em toda a UE e seria ineficaz para garantir a segurança e a proteção dos direitos fundamentais e dos valores da União nos diferentes Estados-Membros. A adoção de abordagens nacionais para a resolução dos problemas apenas criaria mais insegurança jurídica e obstáculos e abrandaria a aceitação da inteligência artificial pelo mercado.

Os objetivos da presente proposta podem ser mais bem alcançados a nível da União, evitando assim uma maior fragmentação do mercado único em quadros nacionais

potencialmente contraditórios que impeçam a livre circulação dos produtos e dos serviços que integram inteligência artificial. Um quadro regulamentar europeu sólido para uma inteligência artificial de confiança também assegurará condições de concorrência equitativas e protegerá todos os cidadãos, reforçando ao mesmo tempo a competitividade e a base industrial da Europa neste domínio. Só uma ação comum a nível da União pode proteger também a soberania digital da União e tirar partido dos seus instrumentos e poderes regulamentares para moldar as regras e as normas mundiais.

2.3.Proporcionalidade

A proposta tem por base os atuais quadros jurídicos e é proporcionada e necessária para alcançar os objetivos a que se propõe, uma vez que segue uma abordagem baseada no risco e impõe encargos regulamentares apenas quando é provável que um sistema de IA represente riscos elevados para os direitos fundamentais e a segurança. Por outro lado, no caso dos sistemas de IA que não são de risco elevado, apenas são impostas obrigações de transparência bastante limitadas, por exemplo, no que diz respeito à prestação de informações para sinalizar a utilização de um sistema de IA quando este interage com seres humanos. No caso dos sistemas de IA de risco elevado, os requisitos relativos à elevada qualidade dos dados, à documentação e à rastreabilidade, à transparência, à supervisão humana, à exatidão e à solidez são estritamente necessários para atenuar os riscos para os direitos fundamentais e a segurança colocados pela inteligência artificial e que não abrangidos por outros quadros jurídicos existentes. As normas harmonizadas e as orientações de apoio, bem como as ferramentas de conformidade, auxiliarão os fornecedores e os utilizadores no cumprimento dos requisitos estabelecidos pela proposta e na minimização dos seus custos. Os custos incorridos pelos operadores são proporcionados aos objetivos alcançados e aos benefícios económicos e reputacionais que os operadores podem esperar desta proposta.

2.4.Escolha do instrumento

A escolha de um regulamento como instrumento jurídico justifica-se pela necessidade de aplicar uniformemente as novas regras, como a definição de inteligência artificial, a proibição de determinadas práticas prejudiciais possibilitadas pela IA e a classificação de determinados sistemas de IA. A aplicabilidade direta de um regulamento, em conformidade com o artigo 288.º do TFUE, reduzirá a fragmentação jurídica e facilitará o desenvolvimento de um mercado único para sistemas de IA legítimos, seguros e de confiança. Para isso, introduzirá um conjunto harmonizado de requisitos básicos no que diz respeito aos sistemas de IA classificados como de risco elevado, bem como obrigações aplicáveis aos fornecedores e aos utilizadores desses sistemas, melhorará a proteção dos direitos fundamentais e proporcionará segurança jurídica para os operadores e os consumidores.

Ao mesmo tempo, as disposições do regulamento não são excessivamente prescritivas e deixam margem a diferentes níveis de ação por parte dos Estados-Membros em termos de elementos que não comprometem os objetivos da iniciativa, em particular a organização interna do sistema de fiscalização do mercado e a adoção de medidas que visam promover a inovação.

3.RESULTADOS DAS AVALIAÇÕES EX POST, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

3.1. Consulta das partes interessadas

A presente proposta é resultado de uma consulta extensiva das principais partes interessadas, na qual a Comissão aplicou os princípios gerais e as normas mínimas de consulta das partes interessadas.

Em 19 de fevereiro de 2020, foi lançada, juntamente com a publicação do Livro Branco sobre a inteligência, artificial uma consulta pública em linha, que decorreu até 14 de junho de 2020. O objetivo dessa consulta era recolher pontos de vista e opiniões sobre o Livro Branco. A consulta visou todas as partes interessadas dos setores público e privado, incluindo administrações públicas, autoridades locais, organizações comerciais e não comerciais, parceiros sociais, peritos, académicos e cidadãos. Uma vez analisadas as respostas recebidas, a Comissão publicou uma síntese dos resultados e as respostas individuais no seu sítio Web 22 .

No total, foram recebidos 1 215 contributos, dos quais 352 de empresas ou organizações/associações comerciais, 406 de cidadãos (92 % eram cidadãos da UE), 152 em nome de instituições académicas/de investigação e 73 de autoridades públicas. As opiniões da sociedade civil foram representadas por 160 respondentes (9 dos quais eram organizações de consumidores, 129 eram organizações não governamentais e 22 eram sindicatos), sendo que 72 respondentes contribuíram identificando-se como «Outros». Das 352 empresas e representantes da indústria, 222 eram empresas e representantes comerciais, sendo que 41,5 % eram micro, pequenas e médias empresas. As restantes eram associação empresariais. De um modo geral, 84 % das respostas das empresas e da indústria eram provenientes da UE-27. Dependendo da pergunta, entre 81 e 598 dos respondentes utilizaram a opção de texto livre para inserir observações. Foram apresentadas mais de 450 posições escritas através do portal EU Survey, quer como complemento das respostas aos inquéritos (mais de 400), quer como contributos autónomos (mais de 50).

De uma forma geral, existe consenso entre as partes interessadas quanto à necessidade de agir. Uma grande maioria das partes interessadas concorda que existem lacunas legislativas ou que é necessária nova legislação. Contudo, várias partes interessadas alertaram a Comissão para a necessidade de evitar duplicação, obrigações contraditórias e excesso de regulamentação. Houve vários comentários a sublinhar a importância de um quadro regulamentar tecnologicamente neutro e proporcionado.

De uma forma geral, as partes interessadas solicitaram uma definição estreita, clara e precisa de «inteligência artificial». As partes interessadas também sublinharam que, além da clarificação do termo «inteligência artificial», é importante definir os termos «risco», «risco elevado», «risco baixo», «identificação biométrica à distância» e «prejuízo/dano». A maioria dos respondentes manifestou-se explicitamente a favor da abordagem baseada no risco. A utilização de um quadro baseado no risco foi considerada uma opção melhor do que aplicar uma regulamentação generalizada a todos os sistemas de IA. Os tipos de riscos e ameaças devem ser baseados numa abordagem setorial e casuística. Os riscos também devem ser calculados tendo em conta o impacto nos direitos e na segurança.

Os ambientes de testagem da regulamentação podem ser bastante úteis para a promoção da IA e são acolhidos com agrado por determinadas partes interessadas, especialmente as associações empresariais.

Entre as partes interessadas que manifestaram a sua opinião sobre os modelos de execução, mais de 50 %, sobretudo entre as associações comerciais, mostraram-se a favor da combinação de uma autoavaliação de riscos ex ante e de uma execução ex post aplicável aos sistemas de IA de risco elevado.

3.2. Obtenção e utilização de competências especializadas

A proposta tem como base dois anos de análise e estreita cooperação das partes interessadas, incluindo académicos, empresas, parceiros sociais, organizações não governamentais, Estados-Membros e cidadãos. O trabalho preparatório foi iniciado em 2018 com a criação de um grupo de peritos de alto nível (GPAN) sobre a IA com uma composição inclusiva e ampla de 52 peritos bem conhecidos incumbidos de prestar aconselhamento à Comissão sobre a aplicação da estratégia da Comissão para a inteligência artificial. Em abril de 2019, a Comissão manifestou o seu apoio 23 aos requisitos essenciais estabelecidos nas «Orientações éticas para uma IA de confiança» do GPAN 24 , que tinham sido revistos para ter em conta mais de 500 observações das partes interessadas. Os requisitos essenciais refletem uma abordagem generalizada e comum segundo a qual o desenvolvimento e a utilização da IA se devem pautar por determinados princípios essenciais orientados por valores, conforme comprovado por um conjunto de códigos e princípios éticos desenvolvidos por várias organizações privadas e públicas de dentro e fora da Europa. A lista de avaliação para uma inteligência artificial de confiança 25 tornou esses requisitos operacionais num processo piloto que incluiu mais de 350 organizações.

Além disso, foi criada a Aliança da IA 26 , uma plataforma onde aproximadamente 4 000 partes interessadas podem debater as implicações tecnológicas e sociais da IA, culminando numa assembleia de IA anual.

O Livro Branco sobre a inteligência artificial desenvolveu esta abordagem inclusiva, incitando as observações de mais de 1 250 partes interessadas, incluindo mais de 450 posições escritas. Consequentemente, a Comissão publicou uma avaliação de impacto inicial que, por sua vez, deu origem a mais de 130 observações 27 . Também foram organizadas outras sessões de trabalho e eventos para as partes interessadas cujos resultados apoiam a análise da avaliação de impacto e as escolhas políticas efetuadas na presente proposta 28 . Foi ainda encomendado um estudo externo para contribuir para a avaliação de impacto.

3.3. Avaliação de impacto

Em consonância com a sua política «Legislar melhor», a Comissão realizou uma avaliação de impacto para a presente proposta, que foi analisada pelo Comité de Controlo da Regulamentação da Comissão. Foi realizada uma reunião com o Comité de Controlo da Regulamentação, em 16 de dezembro de 2020, à qual se seguiu um parecer negativo.

Após uma revisão substancial da avaliação de impacto para ter em conta as observações e uma nova apresentação da avaliação de impacto, o Comité de Controlo da Regulamentação emitiu um parecer positivo em 21 de março de 2021. O anexo 1 da

avaliação de impacto inclui os pareceres do Comité de Controlo da Regulamentação, as recomendações deste e uma explicação sobre como foram tidas em conta.

A Comissão estudou diversas opções políticas para alcançar o objetivo geral da proposta, que consiste em assegurar o correto funcionamento do mercado único, criando condições para o desenvolvimento e a utilização de uma inteligência artificial de confiança na União.

Foram avaliadas quatro opções políticas com diferentes graus de intervenção regulamentar:

- Opção 1: um instrumento legislativo da UE que criasse um regime de rotulagem voluntária;
- Opção 2: uma abordagem ad hoc a nível setorial;
- Opção 3: um instrumento legislativo horizontal da UE que seguisse uma abordagem baseada no risco proporcionada;
- Opção 3+: um instrumento legislativo horizontal da UE que seguisse uma abordagem baseada no risco proporcionada, completada por códigos de conduta para os sistemas de IA que não são de risco elevado;
- Opção 4: um instrumento legislativo horizontal da UE que estabelecesse requisitos obrigatórios para todos os sistemas de IA, independentemente do risco que representam.

De acordo com a metodologia estabelecida da Comissão, cada opção política foi avaliada tendo em conta os impactos económicos e sociais, com particular ênfase nos impactos nos direitos fundamentais. É dada preferência à opção 3+, um quadro regulamentar apenas aplicável aos sistemas de IA de risco elevado, com a possibilidade de todos os fornecedores de sistemas de IA que não são de risco elevado seguirem um código de conduta. Os requisitos dirão respeito aos dados, à documentação e à rastreabilidade, à prestação de informações e à transparência, à supervisão humana, à exatidão e à solidez e seriam obrigatórios para os sistemas de IA de risco elevado. As empresas que introduzam códigos de conduta para outros sistemas de IA fá-lo-ão de modo voluntário.

A opção preferida foi considerada adequada para alcançar mais eficazmente os objetivos da presente proposta. Ao exigir um conjunto de ações, restrito mas eficaz, por parte dos fornecedores e utilizadores de inteligência artificial, a opção preferida limita os riscos de violação dos direitos fundamentais e da segurança dos cidadãos e promove a supervisão e a execução eficazes, ao associar os requisitos apenas aos sistemas em que existe um risco elevado de ocorrência dessas violações. Consequentemente, essa opção mantém os custos de conformidade num valor mínimo, evitando assim um abrandamento desnecessário da adoção da tecnologia devido a preços e custos de conformidade mais elevados. De modo a excluir as possíveis desvantagens para as PME, esta opção inclui inúmeras disposições para apoiar a conformidade e reduzir os respetivos custos, incluindo a criação de ambientes de testagem da regulamentação e a obrigação de ter em conta os interesses das PME aquando da fixação de taxas a pagar pela avaliação da conformidade.

A opção preferida aumentará a confiança dos cidadãos na inteligência artificial, as empresas beneficiarão de maior segurança jurídica e os Estados-Membros não terão qualquer motivo para tomarem uma ação unilateral que possa fragmentar o mercado único. Em resultado de uma maior procura motivada por uma maior confiança, do

aumento da disponibilidade das ofertas devido à segurança jurídica e da ausência de obstáculos ao movimento transfronteiras de sistemas de IA, o mercado único da inteligência artificial irá provavelmente florescer. A União Europeia continuará a desenvolver um ecossistema de inteligência artificial em rápido crescimento, com serviços e produtos inovadores que integram a tecnologia de IA ou sistemas de IA autónomos, o que conduz a um aumento da autonomia digital.

As empresas ou autoridades públicas que desenvolvam ou utilizem aplicações de IA que representam um risco elevado para a segurança ou para os direitos fundamentais dos cidadãos terão de cumprir requisitos e obrigações específicos. O cumprimento destes requisitos implicaria, para o fornecimento de um sistema de IA de risco elevado de gama média com um preço aproximado de 170 000 EUR, custos de aproximadamente 6 000 EUR a 7 000 EUR até 2025. No caso dos utilizadores de inteligência artificial, haveria ainda o custo anual pelo tempo despendido a garantir a supervisão humana, sempre que adequado, dependendo do caso de utilização. Esses custos foram estimados em aproximadamente 5 000 EUR a 8 000 EUR por ano. Os custos de verificação podem corresponder a mais 3 000 EUR a 7 500 EUR no caso dos fornecedores de IA de risco elevado. As empresas ou autoridades públicas que desenvolvam ou utilizem aplicações de IA que não sejam consideradas de risco elevado apenas terão obrigações mínimas de informação. Contudo, estas empresas ou autoridades podem escolher juntar-se a outros e, em conjunto, adotar um código de conduta para seguir requisitos adequados e garantir que os seus sistemas de IA sejam de confiança. Nesse caso, os custos seriam, no máximo, tão elevados quanto os custos impostos aos sistemas de IA de risco elevado, mas provavelmente inferiores.

Os impactos das opções políticas nas diferentes categorias de partes interessadas (operadores económicos/empresas; organismos de avaliação da conformidade, organismos de normalização e outros organismos públicos; indivíduos/cidadãos; investigadores) são descritos pormenorizadamente no anexo 3 da avaliação de impacto que fundamenta a presente proposta.

3.4. Adequação e simplificação da regulamentação

A presente proposta estabelece obrigações que serão aplicáveis aos fornecedores e aos utilizadores de sistemas de IA de risco elevado. No caso dos fornecedores que desenvolvem e colocam esses sistemas no mercado da União, a proposta criará segurança jurídica e assegurará a ausência de obstáculos ao fornecimento transfronteiros de produtos e serviços baseados na IA. No caso das empresas que utilizam a IA, promoverá a confiança entre os seus clientes. No caso das administrações públicas nacionais, esta opção promoverá a confiança pública na utilização da IA e reforçará os mecanismos de execução (mediante a introdução de um mecanismo de coordenação europeu, do fornecimento das capacidades adequadas e da facilitação das auditorias dos sistemas de IA com a aplicação de novos requisitos relacionados com a documentação, a rastreabilidade e a transparência). Além disso, o quadro estipulará medidas específicas para apoiar a inovação, incluindo ambientes de testagem da regulamentação e medidas específicas para ajudar os utilizadores e os fornecedores de pequena dimensão de sistemas de IA de risco elevado a cumprirem as novas regras.

A proposta também visa especificamente o reforço da competitividade e da base industrial da Europa no domínio da inteligência artificial. É assegurada uma coerência completa

com a legislação setorial da União aplicável aos sistemas de IA (por exemplo, em matéria de produtos e serviços) que trará maior clareza e simplificará a execução das novas regras.

3.5. Direitos fundamentais

Dadas as suas características específicas (por exemplo, a opacidade, a complexidade, a dependência dos dados, o comportamento autónomo), a utilização da inteligência artificial pode afetar negativamente um conjunto de direitos fundamentais consagrados na Carta dos Direitos Fundamentais da UE (a seguir designada por «Carta»). A presente proposta procura assegurar um nível elevado de proteção desses direitos fundamentais e visa fazer face aos vários riscos mediante uma abordagem baseada no risco claramente definida.

Graças a um conjunto de requisitos relativos a uma IA de confiança e obrigações proporcionadas para todos os participantes da cadeia de valor, a proposta melhorará e promoverá a proteção dos direitos consagrados na Carta: o direito à dignidade do ser humano (artigo 1.º), o respeito pela vida privada e familiar e a proteção de dados pessoais (artigos 7.º e 8.º), a não discriminação (artigo 21.º) e a igualdade entre homens e mulheres (artigo 23.º). A proposta pretende evitar um efeito inibidor nos direitos à liberdade de expressão (artigo 11.º) e à liberdade de reunião (artigo 12.º), garantir a proteção do direito à ação e a um tribunal imparcial e dos direitos de presunção de inocência e de defesa (artigos 47.º e 48.º), bem como do direito a uma boa administração.

Além disso, conforme aplicável em determinados domínios, a proposta afetará de forma positiva os direitos de um conjunto de grupos especiais, como os direitos dos trabalhadores a condições de trabalho justas e equitativas (artigo 31.º), o direito a um elevado nível de defesa dos consumidores (artigo 28.º), os direitos das crianças (artigo 24.º) e o direito de integração das pessoas com deficiência (artigo 26.º). O direito a um elevado nível de proteção do ambiente e melhoria da sua qualidade (artigo 37.º) também é relevante, incluindo em relação à saúde e à segurança dos cidadãos.

As obrigações relativas à testagem ex ante, à gestão de riscos e à supervisão humana também facilitarão o respeito de outros direitos fundamentais, graças à minimização do risco de decisões assistidas por IA erradas ou enviesadas em domínios críticos como a educação e a formação, o emprego, serviços essenciais, a manutenção da ordem pública e o sistema judicial. Caso continuem a ocorrer violações dos direitos fundamentais, as pessoas afetadas têm acesso a vias eficazes de recurso graças à garantia da transparência e da rastreabilidade dos sistemas de IA, associadas a fortes controlos ex post.

A presente proposta impõe algumas restrições à liberdade de empresa (artigo 16.º) e à liberdade das artes e das ciências (artigo 13.º), a fim de assegurar o cumprimento de razões imperativas de reconhecido interesse público, como a saúde, a segurança, a defesa dos consumidores e a proteção de outros direitos fundamentais («inovação responsável») em caso de desenvolvimento e utilização de tecnologia de IA de risco elevado. Essas restrições são proporcionadas e limitadas ao mínimo necessário para prevenir e atenuar riscos de segurança graves e possíveis violações dos direitos fundamentais.

O aumento das obrigações de transparência também não afetará desproporcionadamente o direito à proteção da propriedade intelectual (artigo 17.º, n.º 2), uma vez que estarão limitadas às informações mínimas necessárias para as pessoas singulares exercerem o seu direito à ação e à transparência necessária perante as autoridades de supervisão e

execução, em conformidade com os mandatos destas. Qualquer divulgação de informações será realizada de acordo com a legislação aplicável, incluindo a Diretiva (UE) 2016/943 relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais. Quando precisam de obter acesso a informações confidenciais ou a código-fonte para analisarem o cumprimento das obrigações substanciais, as autoridades públicas e os organismos notificados ficam sujeitos a obrigações de confidencialidade vinculativas.

4.INCIDÊNCIA ORÇAMENTAL

Os Estados-Membros serão obrigados a designar autoridades de controlo responsáveis pela aplicação dos requisitos legislativos. A sua função de controlo pode ter como base mecanismos existentes, por exemplo, relativos aos organismos de avaliação da conformidade ou à fiscalização do mercado, mas exigirá conhecimentos tecnológicos e recursos humanos e financeiros suficientes. Em função da estrutura preexistente em cada Estado-Membro, este valor pode variar entre 1 e 25 equivalentes a tempo completo por Estado-Membro.
É disponibilizada uma panorâmica pormenorizada dos custos na «ficha financeira» anexa à presente proposta.

5.OUTROS ELEMENTOS

5.1. Planos de execução e acompanhamento, avaliação e prestação de informações

A criação de um mecanismo de acompanhamento e avaliação sólido é crucial para garantir que a proposta seja eficaz para alcançar os seus objetivos específicos. A Comissão ficará responsável por acompanhar os efeitos da proposta e criará um sistema para registar aplicações de IA de risco elevado autónomas numa base de dados pública à escala europeia. Este registo também permitirá que as autoridades competentes, os utilizadores e outras pessoas interessadas verifiquem se o sistema de IA de risco elevado cumpre os requisitos estabelecidos na proposta e exerçam uma maior supervisão dos sistemas de IA que representam riscos elevados para os direitos fundamentais. Para alimentar esta base de dados, os fornecedores de IA serão obrigados a prestar informações importantes sobre os seus sistemas e a apresentar a avaliação da conformidade desses sistemas.

Além disso, os fornecedores de IA serão obrigados a informar as autoridades nacionais competentes sobre incidentes graves ou anomalias que constituam infrações às obrigações em matéria de direitos fundamentais assim que tomarem conhecimento das mesmas, bem como sobre eventuais recolhas ou retiradas de sistemas de IA do mercado. As autoridades nacionais competentes investigarão, subsequentemente, os incidentes/anomalias, recolherão todas as informações necessárias e transmitirão regularmente essas informações à Comissão, incluindo metadados adequados. A Comissão completará estas informações sobre os incidentes por meio de uma análise abrangente do mercado global da inteligência artificial.
A Comissão publicará um relatório de avaliação e reexame do quadro para a inteligência artificial proposto no prazo de cinco anos a contar da data da sua aplicação.

5.2. Explicação pormenorizada das disposições específicas da proposta

5.2.1. ÂMBITO E DEFINIÇÕES (TÍTULO I)
O título I define o objeto do regulamento e o âmbito das novas regras que abrangem a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA. Também estabelece as definições utilizadas no instrumento. A definição de «sistema de IA» constante do quadro jurídico pretende ser o mais tecnologicamente neutra e preparada para o futuro possível, tendo em conta a rápida evolução tecnológica e de mercado no domínio da inteligência artificial. De modo a garantir a segurança jurídica necessária, o título I é completado pelo anexo I, que inclui uma lista pormenorizada de abordagens e técnicas de desenvolvimento de inteligência artificial, que a Comissão adaptará em conformidade com as novas evoluções tecnológicas. São também claramente definidos os participantes essenciais da cadeia de valor no domínio da IA, como os fornecedores e os utilizadores de sistemas de IA, abrangendo os operadores públicos e privados, de modo que assegure condições de concorrência equitativas.

5.2.2. PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS (TÍTULO II)
O título II estabelece uma lista de práticas de IA proibidas. O regulamento segue uma abordagem baseada no risco e diferencia entre as utilizações de IA que criam: i) um risco inaceitável, ii) um risco elevado, iii) um risco baixo ou mínimo. A lista de práticas proibidas do título II inclui todos os sistemas de IA cuja utilização seja considerada inaceitável por violar os valores da União, por exemplo, por violar os direitos fundamentais. As proibições abrangem práticas com potencial significativo para manipular as pessoas por meio de técnicas subliminares que lhes passam despercebidas ou explorar as vulnerabilidades de grupos específicos, como as crianças ou as pessoas com deficiência, para distorcer substancialmente o seu comportamento de uma forma que seja suscetível de causar danos psicológicos ou físicos a essa ou a outra pessoa. Outras práticas manipuladoras ou exploratórias que são possibilitadas pelos sistemas de IA e que afetam os adultos podem ser abrangidas pela legislação em matéria de proteção de dados, de defesa dos consumidores e de serviços digitais, que garante que as pessoas singulares sejam devidamente informadas e tenham a liberdade de decidir não se sujeitar a uma definição de perfis ou a outras práticas que possam afetar o seu comportamento. A proposta também proíbe a classificação social assente na IA para uso geral por parte das autoridades públicas. Por último, é igualmente proibida a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, a não ser que se apliquem determinadas exceções limitadas.

5.2.3. SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO (TÍTULO III)
O título III inclui regras específicas relativas aos sistemas de IA que criam um risco elevado para a saúde e a segurança ou para os direitos fundamentais de pessoas singulares. Em conformidade com uma abordagem baseada no risco, esses sistemas de IA de risco elevado são autorizados no mercado europeu, mas estão sujeitos ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade ex ante. A classificação de um sistema de IA como de risco elevado tem como base a finalidade prevista desse sistema, em conformidade com a atual legislação relativa à segurança dos produtos. Como tal, classificar um sistema como de risco elevado não depende só da função do sistema de IA, mas também da finalidade específica e das modalidades para as quais aquele sistema é utilizado.

O título III, capítulo 1, estabelece as regras de classificação e identifica duas categorias principais de sistemas de IA de risco elevado:

- sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que estão sujeitos a uma avaliação da conformidade ex ante por terceiros,
- outros sistemas de IA autónomos com implicações em matéria de direitos fundamentais que são explicitamente mencionados no anexo III.

A lista de sistemas de IA de risco elevado constante do anexo III inclui um número limitado de sistemas de IA cujos riscos já se materializaram ou são suscetíveis de se materializar num futuro próximo. A fim de garantir que o regulamento possa ser ajustado a novas utilizações e aplicações de IA, a Comissão pode alargar a lista de sistemas de IA de risco elevado utilizados em determinados domínios predefinidos, mediante a aplicação de um conjunto de critérios e de uma metodologia de avaliação de riscos.

O capítulo 2 estabelece os requisitos legais aplicáveis aos sistemas de IA de risco elevado relativamente aos dados e à governação de dados, à documentação e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à segurança. Os requisitos mínimos propostos já são habituais para muitos operadores diligentes e resultam de um trabalho preparatório de dois anos, decorrente das Orientações Éticas do GPAN 29 , aplicado numa fase-piloto por mais de 350 organizações 30 . Também são amplamente coerentes com outras recomendações e princípios internacionais, o que assegura que o quadro para inteligência artificial proposto seja compatível com os adotados pelos parceiros comerciais internacionais da UE. As soluções técnicas específicas para garantir o cumprimento desses requisitos podem, mediante o critério do fornecedor do sistema de IA, derivar de normas ou de outras especificações técnicas ou ser desenvolvidas de acordo com conhecimentos gerais de engenharia ou científicos. Esta flexibilidade é particularmente importante, porque permite que os fornecedores de sistemas de IA escolham o método de cumprimento dos requisitos, tendo em conta os progressos científicos e tecnológicos de ponta neste domínio.

O capítulo 3 indica um conjunto evidente de obrigações horizontais impostas aos fornecedores de sistemas de IA de risco elevado. Também são impostas obrigações proporcionadas aos utilizadores e a outros participantes de toda a cadeia de valor da IA (por exemplo, importadores, distribuidores, mandatários).

O capítulo 4 estabelece o quadro aplicável aos organismos notificados que participam como terceiros independentes nos procedimentos de avaliação da conformidade, ao passo que o capítulo 5 explica pormenorizadamente os procedimentos de avaliação da conformidade que devem ser seguidos para cada tipo de sistema de IA de risco elevado.

A abordagem da avaliação da conformidade visa minimizar os encargos impostos aos operadores económicos e aos organismos notificados, cujas capacidades devem ser progressivamente reforçadas ao longo do tempo. Os sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que são regulamentados por atos do novo quadro legislativo (por exemplo, máquinas, brinquedos, dispositivos médicos, etc.) serão sujeitos aos mesmos mecanismos de conformidade e execução ex ante e ex post aplicáveis aos produtos dos quais são um componente. A

principal diferença é que os mecanismos de ex ante e ex post assegurarão o cumprimento não só dos requisitos estabelecidos pela legislação setorial, mas também dos requisitos estabelecidos pelo presente regulamento.

No que diz respeito aos sistemas de IA de risco elevado autónomos que são mencionados no anexo III, será criado um novo sistema de conformidade e execução. É seguido o modelo do novo quadro legislativo, em que a avaliação é efetuada por meio de controlos internos realizados pelos fornecedores, à exceção dos sistemas de identificação biométrica à distância, que serão sujeitos a uma avaliação da conformidade por terceiros.

Uma avaliação da conformidade ex ante abrangente por meio de controlos internos, aliada a uma forte execução ex post, poderá constituir uma solução eficaz e razoável para esses sistemas, dada a fase inicial da intervenção regulamentar e o facto de o setor da inteligência artificial ser bastante inovador e de só agora estarem a ser reunidos conhecimentos especializados para as auditorias. Uma avaliação dos sistemas de IA de risco elevado autónomos por meio de controlos internos exigirá o cumprimento ex ante completo, eficaz e devidamente documentado de todos os requisitos do regulamento e a conformidade com sistemas sólidos de gestão de riscos e da qualidade e de acompanhamento pós-comercialização. Depois de ter efetuado a avaliação da conformidade necessária, o fornecedor deve registar esses sistemas de IA de risco elevado autónomos numa base de dados da UE que será gerida pela Comissão, a fim de aumentar a transparência e a supervisão públicas e de reforçar a supervisão ex post por parte das autoridades competentes. Por outro lado, por motivos de coerência com a atual legislação relativa à segurança dos produtos, as avaliações da conformidade dos sistemas de IA que são componentes de segurança de produtos seguirão um sistema baseado em procedimentos de avaliação da conformidade por terceiros já estabelecidos nessa legislação setorial relativa à segurança dos produtos. Serão necessárias novas avaliações da conformidade ex ante em caso de modificações substanciais dos sistemas de IA (nomeadamente alterações que excedam o que foi predeterminado pelo fornecedor na documentação técnica e verificado no momento da avaliação da conformidade ex ante inicial).

5.2.4.OBRIGAÇÕES DE TRANSPARÊNCIA APLICÁVEIS A DETERMINADOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL (TÍTULO IV)

O título IV abrange determinados sistemas de IA para ter em conta os riscos específicos que a manipulação dos mesmos representa. Aplicar-se-ão obrigações de transparência aos sistemas que: i) interagem com seres humanos, ii) são utilizados para detetar emoções ou determinar a associação com categorias (sociais) com base ems dados biométricos, iii) geram ou manipulam conteúdos («falsificações profundas»). As pessoas devem ser informadas quando interagem com um sistema de IA ou as suas emoções ou características são reconhecidas por meios automatizados. Se um sistema de IA for utilizado para gerar ou manipular conteúdos de imagem, áudio ou vídeo consideravelmente semelhantes a conteúdos autênticos, deve ser obrigatório divulgar que os conteúdos são gerados por meios automatizados, sob reserva de exceções para fins legítimos (manutenção da ordem pública, liberdade de expressão). Deste modo, as pessoas podem tomar decisões informadas ou distanciar-se de determinadas situações.

5.2.5.MEDIDAS DE APOIO À INOVAÇÃO (TÍTULO V)

O título V contribui para o objetivo de criar um quadro jurídico inovador, preparado para o futuro e resistente a perturbações. Para tal, as autoridades nacionais competentes são

incentivadas a criar ambientes de testagem da regulamentação. Além disso, é criado um quadro básico no que diz respeito à governação, à supervisão e à responsabilidade. Os ambientes de testagem da regulamentação da IA criam um ambiente controlado para testar tecnologias inovadoras durante um período limitado com base num plano de testagem acordado com as autoridades competentes. O título V também inclui medidas para reduzir os encargos regulamentares impostos às PME e às empresas em fase de arranque.

5.2.6.GOVERNAÇÃO E EXECUÇÃO (TÍTULOS VI, VII E VII)
O título VI cria os sistemas de governação a nível da União e nacional. A nível da União, a proposta cria um Comité Europeu para a Inteligência Artificial (a seguir designado por «Comité»), composto por representantes dos Estados-Membros e da Comissão. O Comité facilitará uma aplicação simples, eficaz e harmonizada do presente regulamento, contribuindo para a cooperação eficaz entre as autoridades nacionais de controlo e a Comissão e prestando aconselhamento e conhecimentos especializados à Comissão. O Comité irá ainda recolher e partilhar informações sobre boas práticas entre os Estados-Membros.

A nível nacional, os Estados-Membros terão de designar uma ou mais autoridades nacionais competentes e, entre elas, a autoridade nacional de controlo, para efeitos de supervisão da aplicação e da execução do regulamento. A Autoridade Europeia para a Proteção de Dados atuará como autoridade competente para a supervisão das instituições, órgãos e organismos da União abrangidas pelo âmbito do presente regulamento.

O título VII visa facilitar as atividades de controlo da Comissão e das autoridades nacionais mediante a criação de uma base de dados à escala da UE para os sistemas de IA de risco elevado autónomos com implicações em matéria de direitos fundamentais. A base de dados será gerida pela Comissão e receberá dados dos fornecedores de sistemas de IA, que serão obrigados a registar os seus sistemas antes de os colocar no mercado ou em serviço.

O título VIII estabelece as obrigações de controlo e de comunicação aplicáveis aos fornecedores de sistemas de IA no que diz respeito ao acompanhamento pós-comercialização e à comunicação e investigação de incidentes e anomalias relacionados com a IA. As autoridades de fiscalização do mercado também controlarão o mercado e investigarão o cumprimento das obrigações e dos requisitos aplicáveis a todos os sistemas de IA de risco elevado já colocados no mercado. As autoridades de fiscalização do mercado terão todas as competências previstas no Regulamento (UE) 2019/1020 relativo à fiscalização do mercado. A execução ex post deve assegurar que, após a colocação do sistema de IA no mercado, as autoridades públicas dispõem dos poderes e dos recursos para intervir caso os sistemas de IA criem riscos inesperados que exijam uma ação rápida. As autoridades controlarão ainda o cumprimento das obrigações aplicáveis aos operadores por força do regulamento. A proposta não prevê a criação automática de mais organismos ou autoridades a nível dos Estados-Membros. Como tal, os Estados-Membros podem nomear (e tirar partido dos conhecimentos especializados de) autoridades setoriais existentes, a quem seriam confiados os poderes de controlo e execução das disposições do regulamento.

O acima disposto não prejudica o sistema existente e a repartição de poderes ou a execução ex post das obrigações em matéria de direitos fundamentais nos Estados-

Membros. Quando tal se afigure necessário para cumprirem o seu mandato, as atuais autoridades de supervisão e execução também terão o poder de solicitar e aceder à documentação mantida por força deste regulamento e, caso seja necessário, de solicitar às autoridades de fiscalização do mercado que organizem testes ao sistema de IA de risco elevado por recurso a meios técnicos.

5.2.7.CÓDIGOS DE CONDUTA (TÍTULO IX)

O título IX estabelece um quadro para a criação de códigos de conduta, que visa incentivar os fornecedores de sistemas de IA que não são de risco elevado a aplicar voluntariamente os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado (conforme indicado no título III). Os fornecedores de sistemas de IA que não são de risco elevado podem criar e aplicar autonomamente os códigos de conduta. Esses códigos também podem incluir compromissos voluntários relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento.

5.2.8.DISPOSIÇÕES FINAIS (TÍTULOS X, XI E XII)

O título X salienta a obrigação de todas as partes respeitarem a confidencialidade das informações e dos dados e estabelece regras para o intercâmbio das informações obtidas durante a aplicação do regulamento. O título X também inclui medidas para assegurar a execução eficaz do regulamento por via de sanções efetivas, proporcionadas e dissuasivas aplicáveis a infrações às disposições.

O título XI estabelece as regras para o exercício dos poderes delegados e de execução. A proposta habilita a Comissão a adotar, se for caso disso, atos de execução para garantir a aplicação uniforme do regulamento ou atos delegados para atualizar ou completar as listas constantes dos anexos I a VII.

O título XII incumbe a Comissão de avaliar regularmente a necessidade de atualizar o anexo III e preparar relatórios regulares sobre a avaliação e o reexame do regulamento. Também estabelece disposições finais, incluindo um período de transição diferenciado para a data inicial da aplicação do regulamento, de maneira que facilite uma aplicação simples por todas as partes em causa.

2021/0106 (COD)

Proposta

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,
Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente os artigos 16.º e 114.º,
Tendo em conta a proposta da Comissão Europeia,
Após transmissão do projeto de ato legislativo aos parlamentos nacionais,
Tendo em conta o parecer do Comité Económico e Social Europeu 31 ,
Tendo em conta o parecer do Comité das Regiões 32 ,
Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1)A finalidade do presente regulamento é melhorar o funcionamento do mercado interno mediante o estabelecimento de um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial em conformidade com os valores da União. O presente regulamento observa um conjunto de razões imperativas de reconhecido interesse público, como o elevado nível de proteção da saúde, da segurança e dos direitos fundamentais, e assegura a livre circulação transfronteiras de produtos e serviços baseados em inteligência artificial, evitando assim que os Estados-Membros imponham restrições ao desenvolvimento, à comercialização e à utilização dos sistemas de inteligência artificial, salvo se explicitamente autorizado pelo presente regulamento.

(2)Os sistemas de inteligência artificial (sistemas de IA) podem ser implantados facilmente em vários setores da economia e da sociedade, incluindo além fronteiras, e circular por toda a União. Certos Estados-Membros já ponderaram a adoção de regras nacionais para assegurar que a inteligência artificial seja segura e seja desenvolvida e utilizada em conformidade com as obrigações de proteção dos direitos fundamentais. As diferenças entre regras nacionais podem conduzir à fragmentação do mercado interno e reduzir a segurança jurídica para os operadores que desenvolvem ou utilizam sistemas de IA. Como tal, é necessário assegurar um nível de proteção elevado e coerente em toda a União e evitar divergências que prejudiquem a livre circulação dos sistemas de IA e dos produtos e serviços conexos no mercado interno, mediante o estabelecimento de obrigações uniformes para os operadores e a garantia da proteção uniforme das razões imperativas de reconhecido interesse público e dos direitos das pessoas em todo o mercado interno, com base no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Visto que o presente regulamento contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, é apropriado basear este regulamento no artigo 16.º do TFUE, no

respeitante a essas regras específicas. Face a essas regras específicas e ao recurso ao artigo 16.º do TFUE, é apropriado consultar o Comité Europeu para a Proteção de Dados.

(3)A inteligência artificial é uma família de tecnologias em rápida evolução, capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da inteligência artificial pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na educação e na formação, na gestão das infraestruturas, na energia, nos transportes e logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos e na atenuação das alterações climáticas e adaptação às mesmas.

(4)Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação e utilização específicas, a inteligência artificial pode criar riscos e prejudicar interesses públicos e direitos protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais.

(5)Como tal, é necessário adotar um quadro jurídico da União que estabeleça regras harmonizadas em matéria de inteligência artificial para promover o desenvolvimento, a utilização e a adoção da inteligência artificial no mercado interno e que, ao mesmo tempo, proporcione um nível elevado de proteção de interesses públicos, como a saúde e a segurança e a proteção dos direitos fundamentais, conforme reconhecido e protegido pelo direito da União. Para alcançar esse objetivo, torna-se necessário estabelecer regras aplicáveis à colocação no mercado e à colocação em serviço de determinados sistemas de IA, garantindo assim o correto funcionamento do mercado interno e permitindo que esses sistemas beneficiem do princípio de livre circulação dos produtos e dos serviços. Ao estabelecer essas regras, o presente regulamento apoia o objetivo da União de estar na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança, conforme mencionado pelo Conselho Europeu 33 e garante a proteção de princípios éticos, conforme solicitado especificamente pelo Parlamento Europeu 34 .

(6)A definição de «sistema de IA» deve ser inequívoca, para assegurar a segurança jurídica, concedendo em simultâneo a flexibilidade suficiente para se adaptar a futuras evoluções tecnológicas. A definição deve basear-se nas principais características funcionais do software, em particular a capacidade, tendo em vista um determinado conjunto de objetivos definidos pelos seres humanos, de criar resultados, tais como conteúdos, previsões, recomendações ou decisões que influenciam o ambiente com o qual o sistema interage, quer numa dimensão física, quer digital. Os sistemas de IA podem ser concebidos para operar com diferentes níveis de autonomia e ser utilizados autonomamente ou como componente de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem estar incorporado nele (não integrado). A definição de «sistema de IA» deve ser completada por uma lista de técnicas e abordagens específicas utilizadas para o seu desenvolvimento, que deve ser atualizada face à evolução do mercado e da tecnologia, mediante a adoção de atos delegados da Comissão que alterem essa lista.
(7)A definição de «dados biométricos» utilizada no presente regulamento está em consonância e deve ser interpretada de forma coerente com a definição de «dados

biométricos» constante do artigo 4.º, ponto 14, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho 35 , do artigo 3.º, ponto 18, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho 36 e do artigo 3.º, ponto 13, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho 37 .

(8)O conceito de «sistema de identificação biométrica à distância» utilizado no presente regulamento deve ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que se saiba, antecipadamente, se a pessoa visada estará presente e pode ser identificada, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos utilizados. Tendo em conta as diferentes características e formas como são utilizados, bem como os diferentes riscos inerentes, deve ser efetuada uma distinção entre sistemas de identificação biométrica à distância «em tempo real» e «em diferido». No caso dos sistemas «em tempo real», a recolha dos dados biométricos, a comparação e a identificação ocorrem de imediato, quase de imediato ou, em todo o caso, sem um atraso significativo. Não pode haver, a este respeito, margem para contornar as regras do presente regulamento sobre a utilização «em tempo real» dos sistemas de IA em causa por via da introdução de ligeiros retardamentos no sistema. Os sistemas «em tempo real» implicam a utilização «ao vivo» ou «quase ao vivo» de materiais, como vídeos, criados por uma câmara ou outro dispositivo com uma funcionalidade semelhante. Por outro lado, no caso dos sistemas «em diferido», os dados biométricos já foram recolhidos e a comparação e a identificação ocorrem apenas após um atraso significativo. Estes sistemas utilizam materiais, tais como imagens ou vídeos, criados por câmaras de televisão em circuito fechado ou dispositivos privados antes de o sistema ser utilizado relativamente às pessoas singulares em causa.

(9)Para efeitos do presente regulamento, deve entender-se por «espaço acessível ao público» qualquer espaço físico que seja acessível ao público, independentemente de o espaço em questão ser detido por uma entidade privada ou pública. Como tal, a definição não abrange locais de natureza privada ou que não são de acesso livre a terceiros, incluindo as autoridades policiais, a não ser que essas partes tenham sido especificamente convidadas ou autorizadas, tais como residências, clubes privados, escritórios, armazéns e fábricas. Os espaços em linha também não são abrangidos, uma vez que não são espaços físicos. Contudo, a mera possibilidade de aplicar determinadas condições para o acesso a um espaço particular, como bilhetes de admissão ou restrições de idade, não significa que o espaço não é acessível ao público na aceção do presente regulamento. Consequentemente, além dos espaços públicos, como as ruas, as partes relevantes dos edifícios governamentais e a maioria das infraestruturas de transporte, espaços como cinemas, teatros, lojas e centros comerciais também são, por norma, acessíveis ao público. Para determinar se um espaço é acessível ao público deve recorrer-se a uma análise casuística, tendo em conta as especificidades da situação em apreço.

(10)Para assegurar condições de concorrência equitativas e uma proteção eficaz dos direitos e das liberdades das pessoas singulares em toda a União, as regras estabelecidas no presente regulamento devem aplicar-se aos fornecedores de sistemas de IA de uma forma não discriminatória, independentemente de estarem estabelecidos na União ou num país terceiro, e aos utilizadores de sistemas de IA estabelecidos na União.

(11)Face à natureza digital dos sistemas de IA, determinados sistemas devem ser abrangidos pelo âmbito do presente regulamento, mesmo quando não são colocados no mercado ou em serviço, nem são utilizados na União. Esta situação verifica-se, por exemplo, quando um operador estabelecido na União contrata determinados serviços a um operador estabelecido fora da União relativamente a uma atividade a realizar por um sistema de IA que seria considerado «de risco elevado» e cujos efeitos afetam pessoas singulares localizadas na União. Nessas circunstâncias, o operador fora da União poderia utilizar o seu sistema de IA para tratar dados recolhidos e transferidos licitamente da União e fornecer ao operador contratante na União o resultado desse sistema de IA decorrente desse tratamento, sem que o sistema de IA em causa fosse colocado no mercado ou em serviço ou utilizado na União. Para evitar que o presente regulamento seja contornado e para assegurar uma proteção eficaz das pessoas singulares localizadas na União, o presente regulamento deve ser igualmente aplicável a fornecedores e utilizadores de sistemas de IA estabelecidos num país terceiro nos casos em que o resultado desses sistemas seja utilizado na União. No entanto, para ter em conta os mecanismos existentes e as necessidades especiais de cooperação com os parceiros estrangeiros com quem são trocadas informações e dados, o presente regulamento não deve ser aplicável às autoridades públicas de um país terceiro e às organizações internacionais quando estas atuam no âmbito de acordos internacionais celebrados a nível nacional ou europeu para efeitos de cooperação policial e judiciária com a União ou com os seus Estados-Membros. Tais acordos têm sido celebrados bilateralmente entre Estados-Membros e países terceiros ou entre a União Europeia, a Europol e outras agências da UE e países terceiros e organizações internacionais.

(12)O presente regulamento deverá ser também aplicável a instituições, órgãos e organismos da União quando atuam como fornecedor ou utilizador de um sistema de IA. Os sistemas de IA desenvolvidos ou utilizados exclusivamente para efeitos militares devem ser excluídos do âmbito do presente regulamento, caso essa utilização seja abrangida pela competência exclusiva da política externa e de segurança comum regulamentada nos termos do título V do Tratado da União Europeia (TUE). O presente regulamento não prejudica a responsabilidade dos prestadores intermediários de serviços estabelecida na Diretiva 2000/31/CE do Parlamento Europeu e do Conselho [na redação que lhe foi dada pelo Regulamento Serviços Digitais].

(13)A fim de assegurar um nível elevado e coerente de proteção dos interesses públicos nos domínios da saúde, da segurança e dos direitos fundamentais, devem ser criadas normas comuns aplicáveis a todos os sistemas de IA de risco elevado. Essas normas devem ser coerentes com a Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta») e não discriminatórias, bem como estar em consonância com os compromissos comerciais internacionais da União.

(14)Para que o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deve seguir-se uma abordagem baseada no risco claramente definida. Essa abordagem deve adaptar o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos criados pelos sistemas de IA. Como tal, é necessário proibir determinadas práticas de inteligência artificial, estabelecer requisitos aplicáveis aos sistemas de IA de risco elevado e obrigações para os operadores pertinentes, bem como estabelecer obrigações de transparência para determinados sistemas de IA.

(15)Além das inúmeras utilizações benéficas da inteligência artificial, essa tecnologia pode ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e devem ser proibidas, pois desrespeitam valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como direitos fundamentais da União, incluindo o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.

(16) Deve ser proibida a colocação no mercado, a colocação em serviço ou a utilização de determinados sistemas de IA concebidos para distorcer o comportamento humano, os quais são passíveis de provocar danos físicos ou psicológicos. Esses sistemas de IA utilizam componentes subliminares que não são detetáveis pelos seres humanos ou exploram vulnerabilidades de crianças e adultos associadas à sua idade e às suas incapacidades físicas ou mentais. A intenção destes sistemas é distorcer substancialmente o comportamento de uma pessoa de uma forma que cause ou seja suscetível de causar danos a essa ou a outra pessoa. A intenção pode não ser detetada caso a distorção do comportamento humano resulte de fatores externos ao sistema de IA que escapam ao controlo do fornecedor ou do utilizador. A proibição não pode impedir a investigação desses sistemas de IA para efeitos legítimos, desde que essa investigação não implique uma utilização do sistema de IA em relações homem-máquina que exponha pessoas singulares a danos e seja efetuada de acordo com normas éticas reconhecidas para fins de investigação científica.

(17)Os sistemas de IA que possibilitam a classificação social de pessoas singulares para uso geral das autoridades públicas ou em nome destas podem criar resultados discriminatórios e levar à exclusão de determinados grupos. Estes sistemas podem ainda violar o direito à dignidade e à não discriminação e os valores da igualdade e da justiça. Esses sistemas de IA avaliam ou classificam a credibilidade de pessoas singulares com base no seu comportamento social em diversos contextos ou em características de personalidade ou pessoais, conhecidas ou previsíveis. A classificação social obtida por meio desses sistemas de IA pode levar ao tratamento prejudicial ou desfavorável de pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com o contexto nos quais os dados foram originalmente gerados ou recolhidos ou a um tratamento prejudicial que é injustificado ou desproporcionado face à gravidade do seu comportamento social. Como tal, esses sistemas de IA devem ser proibidos.

(18)A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública é considerada particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais.

(19)Como tal, deve ser proibida a utilização desses sistemas para efeitos de manutenção da ordem pública, salvo em três situações enunciadas exaustivamente e definidas de modo restrito, em que a utilização é estritamente necessária por motivos de interesse público

importante e cuja importância prevalece sobre os riscos. Essas situações implicam a procura de potenciais vítimas de crimes, incluindo crianças desaparecidas, certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataque terrorista, e a deteção, localização, identificação ou instauração de ações penais relativamente a infratores ou suspeitos de infrações penais a que se refere a Decisão-Quadro 2002/584/JAI do Conselho 38 , desde que puníveis no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro. Esse limiar para a pena ou medida de segurança privativa de liberdade prevista no direito nacional contribui para assegurar que a infração seja suficientemente grave para justificar potencialmente a utilização de sistemas de identificação biométrica à distância «em tempo real». Além disso, das 32 infrações penais enumeradas na Decisão-Quadro 2002/584/JAI do Conselho, algumas são provavelmente mais pertinentes do que outras, já que o recurso à identificação biométrica à distância «em tempo real» será previsivelmente necessário e proporcionado em graus extremamente variáveis no respeitante à deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito das diferentes infrações penais enumeradas e tendo em conta as prováveis diferenças em termos de gravidade, probabilidade e magnitude dos prejuízos ou das possíveis consequências negativas.

(20)A fim de assegurar que esses sistemas sejam utilizados de uma forma responsável e proporcionada, também importa estabelecer que, em cada uma dessas três situações enunciadas exaustivamente e definidas de modo restrito, é necessário ter em conta determinados elementos, em especial no que se refere à natureza da situação que dá origem ao pedido e às consequências da utilização para os direitos e as liberdades de todas as pessoas em causa e ainda às salvaguardas e condições previstas para a utilização. Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a limites espaciais e temporais adequados, tendo em conta, especialmente, os dados ou indícios relativos às ameaças, às vítimas ou ao infrator. A base de dados de pessoas utilizada como referência deve ser adequada a cada utilização em cada uma das três situações acima indicadas.

(21)Cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a uma autorização expressa e específica de uma autoridade judiciária ou de uma autoridade administrativa independente de um Estado-Membro. Em princípio, essa autorização deve ser obtida antes da sua utilização, salvo em situações de urgência devidamente justificadas, ou seja, quando a necessidade de utilizar os sistemas em causa torna efetiva e objetivamente impossível obter uma autorização antes de iniciar essa utilização. Nessas situações de urgência, a utilização deve limitar-se ao mínimo absolutamente necessário e estar sujeita a salvaguardas e condições adequadas, conforme determinado pelo direito nacional e especificado no contexto de cada caso de utilização urgente pela própria autoridade policial. Ademais, nessas situações, a autoridade policial deve procurar obter quanto antes uma autorização, apresentando as razões para não ter efetuado o pedido mais cedo.

(22)Além disso, no âmbito do quadro exaustivo estabelecido pelo presente regulamento, importa salientar que essa utilização no território de um Estado-Membro apenas deve ser possível uma vez que o Estado-Membro em causa tenha decidido possibilitar

expressamente a autorização dessa utilização de acordo com o presente regulamento nas regras de execução previstas no direito nacional. Consequentemente, ao abrigo do presente regulamento, os Estados-Membros continuam a ser livres de não possibilitar essa utilização ou de apenas possibilitar essa utilização relativamente a alguns dos objetivos passíveis de justificar uma utilização autorizada identificados no presente regulamento.

(23)A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública implica necessariamente o tratamento de dados biométricos. As regras do presente regulamento que proíbem essa utilização, salvo em certas exceções, e que têm por base o artigo 16.º do TFUE, devem aplicar-se como lex specialis relativamente às regras em matéria de tratamento de dados biométricos previstas no artigo 10.º da Diretiva (UE) 2016/680, regulando assim essa utilização e o tratamento de dados biométricos conexo de uma forma exaustiva. Como tal, essa utilização e esse tratamento apenas devem ser possíveis se forem compatíveis com o quadro estabelecido pelo presente regulamento, sem que exista margem, fora desse quadro, para as autoridades competentes utilizarem esses sistemas e efetuarem o tratamento desses dados pelos motivos enunciados no artigo 10.º da Diretiva (UE) 2016/680, caso atuem para efeitos de manutenção da ordem pública. Neste contexto, o presente regulamento não pretende constituir o fundamento jurídico do tratamento de dados pessoais, nos termos do artigo 8.º da Diretiva (UE) 2016/680. Contudo, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para outros fins que não os policiais, incluindo por parte das autoridades competentes, não deve ser abrangida pelo quadro específico relativo a essa utilização para efeitos de manutenção da ordem pública estabelecido pelo presente regulamento. Assim, uma utilização para outros fins que não a manutenção da ordem pública não deve estar sujeita ao requisito de autorização previsto no presente regulamento nem às eventuais regras de execução previstas no direito nacional.

(24)Qualquer tratamento de dados biométricos e de outros dados pessoais envolvidos na utilização de sistemas de IA para fins de identificação biométrica, desde que não estejam associados à utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, conforme regida pelo presente regulamento, incluindo quando esses sistemas são utilizados pelas autoridades competentes em espaços acessíveis ao público para outros fins que não os policiais, deve continuar a cumprir todos os requisitos decorrentes do artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, do artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725 e do artigo 10.º da Diretiva (UE) 2016/680, conforme aplicável.

(25)Nos termos do artigo 6.º-A do Protocolo (n.º 21) relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, a Irlanda não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.os 2 e 3, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito da parte III, título V, capítulos 4 ou 5, do TFUE, caso não esteja vinculada por regras que rejam formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devam ser observadas as disposições definidas com base no artigo 16.º do TFUE.

(26)Nos termos dos artigos 2.º e 2.º-A do Protocolo (n.º 22) relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.os 2 e 3, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, nem fica sujeita à aplicação das mesmas.

(27)Os sistemas de IA de risco elevado só podem ser colocados no mercado da União ou colocados em serviço se cumprirem determinados requisitos obrigatórios. Esses requisitos devem assegurar que os sistemas de IA de risco elevado disponíveis na União ou cujos resultados sejam utilizados na União não representam riscos inaceitáveis para interesses públicos importantes da União, conforme reconhecidos e protegidos pelo direito da União. A classificação de «risco elevado» aplicada a sistemas de IA deve limitar-se aos sistemas que têm um impacto prejudicial substancial na saúde, na segurança e nos direitos fundamentais das pessoas no território da União e essa limitação deve minimizar quaisquer potenciais restrições ao comércio internacional, se for caso disso.

(28)Os sistemas de IA podem produzir resultados adversos para a saúde e a segurança das pessoas, em particular quando esses sistemas funcionam como componentes de produtos. Em conformidade com os objetivos da legislação de harmonização da União, designadamente facilitar a livre circulação de produtos no mercado interno e assegurar que apenas os produtos seguros e conformes entram no mercado, é importante prevenir e atenuar devidamente os riscos de segurança que possam ser criados por um produto devido aos seus componentes digitais, incluindo sistemas de IA. A título de exemplo, os robôs, que se têm tornado cada vez mais autónomos, devem operar com segurança e realizar as suas funções em ambientes complexos, seja num contexto industrial ou de assistência e cuidados pessoais. De igual forma, no setor da saúde, em que os riscos para a vida e a saúde são particularmente elevados, os cada vez mais sofisticados sistemas de diagnóstico e sistemas que apoiam decisões humanas devem produzir resultados exatos e de confiança. A dimensão dos impactos adversos causados pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado. Esses direitos incluem o direito à dignidade do ser humano, o respeito da vida privada e familiar, a proteção de dados pessoais, a liberdade de expressão e de informação, a liberdade de reunião e de associação, a não discriminação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa e o direito a uma boa administração. Além desses direitos, é importante salientar que as crianças têm direitos específicos, consagrados no artigo 24.º da Carta da UE e na Convenção das Nações Unidas sobre os Direitos da Criança (descritos em mais pormenor no Comentário geral n.º 25 da Convenção das Nações Unidas sobre os Direitos da Criança no respeitante ao ambiente digital), que exigem que as vulnerabilidades das crianças sejam tidas em conta e que estas recebam a proteção e os cuidados necessários ao seu bem-estar. O direito fundamental a um nível elevado de proteção do ambiente consagrado na Carta e aplicado nas políticas da União também deve ser tido em conta ao avaliar a gravidade dos danos que um sistema de IA pode causar, incluindo em relação à saúde e à segurança das pessoas.

(29)Relativamente aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo

âmbito do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho 39 , do Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho 40 , do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho 41 , da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho 42 , da Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho 43 , do Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho 44 , do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho 45 e do Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho 46 , é adequado alterar esses atos para assegurar que a Comissão tenha em conta, aquando da adoção de futuros atos delegados ou de execução baseados nesses atos, os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado estabelecidos no presente regulamento, atendendo às especificidades técnicas e regulamentares de cada setor e sem interferir com os mecanismos de governação, de avaliação da conformidade e de execução existentes nem com as autoridades estabelecidas nestes regulamentos.

(30)Relativamente aos sistemas de IA que são componentes de segurança de produtos ou que são, eles próprios, produtos abrangidos pelo âmbito de determinada legislação de harmonização da União, é apropriado classificá-los como de risco elevado ao abrigo do presente regulamento nos casos em que forem objeto de um procedimento de avaliação da conformidade realizado por um organismo terceiro de avaliação da conformidade nos termos dessa legislação de harmonização da União aplicável. Em particular, tais produtos são máquinas, brinquedos, ascensores, aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas, equipamentos de rádio, equipamentos sob pressão, equipamentos de embarcações de recreio, instalações por cabo, aparelhos a gás, dispositivos médicos e dispositivos médicos para diagnóstico in vitro.

(31)Classificar um sistema de IA como de risco elevado nos termos do presente regulamento não implica necessariamente que o produto cujo componente de segurança é o sistema de IA ou que o próprio sistema de IA enquanto produto seja considerado «de risco elevado», segundo os critérios estabelecidos na legislação de harmonização da União aplicável ao produto. Tal verifica-se no respeitante ao Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho 47 e ao Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho 48 , que preveem a avaliação por terceiros da conformidade de produtos de risco médio e elevado.

(32)Relativamente aos sistemas de IA autónomos, ou seja, sistemas de IA de risco elevado que não são componentes de segurança de produtos nem são, eles próprios, produtos, é apropriado classificá-los como de risco elevado se, em função da finalidade prevista, representarem um risco elevado de danos para a saúde e a segurança ou de prejuízo para os direitos fundamentais das pessoas, tendo em conta a gravidade dos possíveis danos e a probabilidade dessa ocorrência, e se forem utilizados num conjunto de domínios especificamente predefinidos no regulamento. A identificação desses sistemas baseia-se na mesma metodologia e nos mesmos critérios previstos para futuras alterações da lista de sistemas de IA de risco elevado.

(33)As imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios. Esta questão é particularmente importante no que diz respeito à idade, à etnia, ao sexo ou a deficiências das pessoas. Como tal, os sistemas de

identificação biométrica à distância «em tempo real» e «em diferido» devem ser classificados como de risco elevado. Face aos riscos que estes dois tipos de sistemas de identificação biométrica à distância representam, ambos devem estar sujeitos a requisitos específicos relativos às capacidades de registo e à supervisão humana.

(34)No tocante à gestão e ao funcionamento de infraestruturas críticas, é apropriado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo do tráfego rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade, uma vez que a falha ou anomalia destes sistemas pode pôr em risco a vida e a saúde das pessoas em larga escala e provocar perturbações substanciais das atividades sociais e económicas normais.

(35)Os sistemas de IA utilizados no domínio da educação ou formação profissional, designadamente para determinar o acesso ou a afetação de pessoas a instituições de ensino e de formação profissional ou para avaliar testes que as pessoas realizam no âmbito da sua educação ou como pré-condição para a mesma, devem ser considerados de risco elevado, uma vez que determinam o percurso académico e profissional das pessoas e, como tal, afetam a capacidade destas para garantir a subsistência. Se indevidamente concebidos e utilizados, estes sistemas podem violar o direito à educação e à formação, bem como o direito a não ser alvo de discriminação e de perpetuação de padrões históricos de discriminação.

(36)Os sistemas de IA utilizados nos domínios do emprego, da gestão de trabalhadores e do acesso ao emprego por conta própria, nomeadamente para efeitos de recrutamento e seleção, de tomada de decisões sobre promoções e despedimentos, de repartição de tarefas e de controlo ou avaliação de pessoas no âmbito de relações contratuais de trabalho também devem ser classificados como de risco elevado, uma vez que podem ter um impacto significativo nas perspetivas de carreira e na subsistência dessas pessoas. O conceito de «relações contratuais relacionadas com o trabalho» deve abranger os funcionários e as pessoas que prestam serviços por intermédio de plataformas, conforme mencionado no programa de trabalho da Comissão para 2021. Em princípio, essas pessoas não devem ser consideradas «utilizadores» na aceção do presente regulamento. Ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoas em relações contratuais relacionadas com o trabalho, esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra as mulheres, certos grupos etários, pessoas com deficiência ou pessoas de uma determinada origem racial ou étnica ou orientação sexual. Os sistemas de IA utilizados para controlar o desempenho e o comportamento destas pessoas podem ter ainda um impacto nos seus direitos à proteção de dados pessoais e à privacidade.

(37)Outro domínio no qual a utilização de sistemas de IA merece especial atenção é o acesso a determinados serviços e prestações essenciais, de cariz privado e público, e o usufruto dos mesmos, os quais são necessários para que as pessoas participem plenamente na sociedade ou melhorem o seu nível de vida. Em particular, os sistemas de IA utilizados para avaliar a classificação de crédito ou a capacidade de endividamento de pessoas singulares devem ser classificados como sistemas de IA de risco elevado, uma vez que determinam o acesso dessas pessoas a recursos financeiros ou a serviços essenciais, como o alojamento, a eletricidade e os serviços de telecomunicações. Os sistemas de IA utilizados para essa finalidade podem conduzir à discriminação de pessoas ou grupos e perpetuar padrões históricos de discriminação, por exemplo, em razão da origem étnica

ou racial, deficiência, idade ou orientação sexual, ou criar novas formas de impactos discriminatórios. Tendo em conta a dimensão bastante limitada do impacto e as alternativas disponíveis no mercado, é apropriado isentar os sistemas de IA utilizados para efeitos de avaliação da capacidade de endividamento e de classificação de crédito que sejam colocados em serviço por fornecedores de pequena dimensão para utilização própria. Normalmente, as pessoas singulares que se candidatam ou que recebem prestações e serviços de assistência pública de autoridades públicas dependem dos mesmos e estão numa posição vulnerável face às autoridades competentes. Caso sejam utilizados para determinar a recusa, redução, revogação ou recuperação dessas prestações e serviços pelas autoridades, os sistemas de IA podem ter um impacto significativo na subsistência das pessoas e podem infringir os seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade do ser humano ou à ação. Como tal, esses sistemas devem ser classificados como de risco elevado. No entanto, o presente regulamento não pode constituir um obstáculo ao desenvolvimento e à utilização de abordagens inovadoras na administração pública, que tirariam partido de uma maior utilização de sistemas de IA conformes e seguros, desde que esses sistemas não representem um risco elevado para as pessoas coletivas e singulares. Por último, os sistemas de IA utilizados para enviar ou estabelecer prioridades no envio de serviços de resposta a emergências devem ser classificados como de risco elevado, uma vez que tomam decisões em situações bastante críticas que afetam a vida, a saúde e os bens das pessoas.

(38)As ações das autoridades policiais que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outros impactos adversos nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de exatidão ou solidez ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode destacar pessoas de uma forma discriminatória ou incorreta e injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados. Como tal, é apropriado classificar como de risco elevado um conjunto de sistemas de IA concebidos para serem utilizados no contexto da manutenção da ordem pública, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar impactos adversos, reter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes. Tendo em conta a natureza das atividades em causa e os riscos associados às mesmas, esses sistemas de IA de risco elevado devem incluir, em particular, sistemas de IA concebidos para serem utilizados pelas autoridades policiais em avaliações individuais de riscos, em polígrafos e em instrumentos semelhantes ou para detetar o estado emocional de uma pessoa singular, para detetar «falsificações profundas», para avaliar a fiabilidade dos elementos de prova em processos penais, para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis de pessoas singulares ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos, para a definição de perfis no decurso da deteção, investigação ou repressão de infrações penais, bem como para o estudo analítico de crimes relativos a pessoas singulares. Os sistemas de IA especificamente concebidos para serem utilizados em processos administrativos por autoridades fiscais e aduaneiras não devem ser considerados sistemas de IA de risco

elevado utilizados por autoridades policiais para efeitos de prevenção, deteção, investigação e repressão de infrações penais.

(39)Os sistemas de IA utilizados na gestão da migração, do asilo e do controlo das fronteiras afetam pessoas que, muitas vezes, se encontram numa posição particularmente vulnerável e que dependem do resultado das ações das autoridades públicas competentes. Como tal, a exatidão, a natureza não discriminatória e a transparência dos sistemas de IA utilizados nesses contextos são particularmente importantes para garantir o respeito dos direitos fundamentais das pessoas em causa, nomeadamente os seus direitos à livre circulação, à não discriminação, à proteção da vida privada e dos dados pessoais, à proteção internacional e a uma boa administração. Deste modo, é apropriado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados por autoridades públicas competentes incumbidas de funções no domínio da gestão da migração, do asilo e do controlo das fronteiras, como polígrafos e instrumentos semelhantes, ou para detetar o estado emocional de uma pessoa singular; para avaliar determinados riscos colocados pelas pessoas singulares que entram no território de um Estado-Membro ou pedem um visto ou asilo; para verificar a autenticidade dos documentos apresentados pelas pessoas singulares; para auxiliar as autoridades públicas competentes na análise dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, com o objetivo de estabelecer a elegibilidade das pessoas singulares que requerem determinado estatuto. Os sistemas de IA no domínio da gestão da migração, do asilo e do controlo das fronteiras abrangidos pelo presente regulamento devem cumprir os requisitos processuais estabelecidos na Diretiva 2013/32/UE do Parlamento Europeu e do Conselho 49 , no Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho 50 e noutra legislação aplicável.

(40)Determinados sistemas de IA concebidos para a administração da justiça e os processos democráticos devem ser classificados como de risco elevado, tendo em conta o seu impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial. Em particular, para fazer face aos riscos de potenciais enviesamentos, erros e opacidade, é apropriado classificar como de risco elevado os sistemas de IA concebidos para auxiliar as autoridades judiciárias na investigação e na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos. Contudo, essa classificação não deve ser alargada aos sistemas de IA concebidos para atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais, como a anonimização ou a pseudonimização de decisões judiciais, documentos ou dados, comunicações entre pessoal, tarefas administrativas ou afetação de recursos.

(41)A classificação de um sistema de IA como de risco elevado por força do presente regulamento não deve ser interpretada como uma indicação de que a utilização do sistema é necessariamente lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União, por exemplo, em matéria de proteção de dados pessoais ou de utilização de polígrafos e de instrumentos semelhantes ou de outros sistemas para detetar o estado emocional de pessoas singulares. Essa utilização deve continuar sujeita ao cumprimento dos requisitos aplicáveis resultantes da Carta e dos atos do direito derivado da União e do direito nacional em vigor. O presente regulamento não pode ser entendido como um fundamento jurídico para o tratamento de dados pessoais, incluindo de categorias especiais de dados pessoais, se for caso disso.

(42)Para atenuar os riscos dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço no mercado da União para os utilizadores e as pessoas afetadas, devem aplicar-se determinados requisitos obrigatórios, tendo em conta a finalidade de utilização prevista do sistema e de acordo com o sistema de gestão de riscos a estabelecer pelo fornecedor.

(43)Os sistemas de IA de risco elevado devem estar sujeitos ao cumprimento de requisitos relativos à qualidade dos conjuntos de dados utilizados, à documentação técnica e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à cibersegurança. Esses requisitos são necessários para atenuar eficazmente os riscos para a saúde, a segurança e os direitos fundamentais, em função da finalidade prevista do sistema e quando não existam outras medidas menos restritivas do comércio, evitando, assim, restrições injustificadas do comércio.

(44)A disponibilidade de dados de elevada qualidade é um fator essencial para o desempenho de vários sistemas de IA, sobretudo quando são utilizadas técnicas que envolvem o treino de modelos, com vista a assegurar que o sistema de IA de risco elevado funcione como pretendido e de modo seguro e não se torne a fonte de uma discriminação proibida pelo direito da União. Para garantir conjuntos de dados de treino, validação e teste de elevada qualidade é necessário aplicar práticas adequadas de governação e gestão de dados. Os conjuntos de dados de treino, validação e teste devem ser suficientemente relevantes, representativos, livres de erros e completos, tendo em vista a finalidade prevista do sistema. Também devem ter as propriedades estatísticas adequadas, nomeadamente no que respeita às pessoas ou aos grupos de pessoas nos quais o sistema de IA de risco elevado será utilizado. Em particular, os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do exigido face à sua finalidade prevista, as características, as funcionalidades ou os elementos que são específicos do ambiente ou do contexto geográfico, comportamental ou funcional no qual o sistema de IA será utilizado. A fim de proteger os direitos de outras pessoas da discriminação que possa resultar do enviesamento dos sistemas de IA, os fornecedores devem poder efetuar também o tratamento de categorias especiais de dados pessoais por motivos de interesse público importante, para assegurar o controlo, a deteção e a correção de enviesamentos em sistemas de IA de risco elevado.

(45)No contexto do desenvolvimento de sistemas de IA de risco elevado, determinados intervenientes, como fornecedores, organismos notificados e outras entidades interessadas, como polos de inovação digital, instalações de teste e experimentação e investigadores, devem poder aceder e utilizar conjuntos de dados de elevada qualidade dentro das respetivas áreas de intervenção relacionadas com o presente regulamento. Os espaços comuns europeus de dados criados pela Comissão e a facilitação da partilha de dados entre empresas e com as administrações públicas por motivos de interesse público serão cruciais para conceder um acesso fiável, responsável e não discriminatório a dados de elevada qualidade para o treino, a validação e o teste de sistemas de IA. Por exemplo, no domínio da saúde, o espaço europeu de dados de saúde facilitará o acesso não discriminatório a dados de saúde e o treino de algoritmos de inteligência artificial com base nesses conjuntos de dados, de forma segura, oportuna, transparente, fidedigna e protetora da privacidade e sob a alçada de uma governação institucional adequada. As autoridades competentes, incluindo as autoridades setoriais, que concedem ou apoiam o

acesso aos dados também podem apoiar o fornecimento de dados de elevada qualidade para fins de treino, validação e teste de sistemas de IA.

(46)Para verificar o cumprimento dos requisitos estabelecidos no presente regulamento, é essencial dispor de informações sobre o desenvolvimento dos sistemas de IA de risco elevado e sobre o seu desempenho ao longo do respetivo ciclo de vida. Tal exige a manutenção de registos e a disponibilização de documentação técnica que contenham as informações necessárias para avaliar o cumprimento, por parte do sistema de IA, dos requisitos aplicáveis. Essas informações devem incluir as características gerais, as capacidades e as limitações do sistema, os algoritmos, os dados e os processos de treino, teste e validação utilizados, bem como documentação sobre o sistema de gestão de riscos aplicado. A documentação técnica deve estar sempre atualizada.

(47)Para fazer face à opacidade que pode tornar determinados sistemas de IA incompreensíveis ou demasiado complexos para as pessoas singulares, os sistemas de IA de risco elevado devem observar um certo grau de transparência. Os utilizadores devem ser capazes de interpretar o resultado do sistema e utilizá-lo de forma adequada. Como tal, os sistemas de IA de risco elevado devem ser acompanhados de documentação pertinente e instruções de utilização e incluir informações concisas e claras, nomeadamente informações relativas a possíveis riscos para os direitos fundamentais e de discriminação, se for caso disso.

(48)Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que permita a sua supervisão por pessoas singulares. Para o efeito, o fornecedor do sistema deve identificar medidas de supervisão humana adequadas antes da colocação no mercado ou da colocação em serviço do sistema. Em particular, se for caso disso, essas medidas devem garantir que o sistema integre restrições operacionais que não possam ser neutralizadas pelo próprio sistema e que respondam ao operador humano e que as pessoas singulares a quem foi atribuída a supervisão humana tenham as competências, a formação e a autoridade necessárias para desempenhar essa função.

(49)Os sistemas de IA de risco elevado devem ter um desempenho coerente ao longo de todo o ciclo de vida e apresentar um nível adequado de exatidão, solidez e cibersegurança, de acordo com o estado da técnica geralmente reconhecido. O nível e as métricas de exatidão devem ser comunicadas aos utilizadores.

(50)A solidez técnica é um requisito essencial dos sistemas de IA de risco elevado. Estes sistemas devem ser resistentes aos riscos associados às suas limitações (por exemplo, erros, falhas, incoerências, situações inesperadas), bem como a ações maliciosas suscetíveis de pôr em causa a segurança do sistema de IA e dar origem a comportamentos prejudiciais ou indesejáveis. A falta de proteção contra estes riscos pode causar problemas de segurança ou afetar negativamente os direitos fundamentais, por exemplo, devido a decisões erradas ou a resultados errados ou enviesados gerados pelo sistema de IA.

(51)A cibersegurança desempenha um papel fundamental para garantir que os sistemas de IA sejam resistentes às ações de terceiros mal-intencionados que tentam explorar as vulnerabilidades dos sistemas com o objetivo de lhes alterar a utilização, o comportamento e o desempenho ou por em causa as propriedades de segurança. Os ciberataques contra sistemas de IA podem tirar partido de ativos específicos de inteligência artificial, como os conjuntos de dados de treino (por exemplo, contaminação

de dados) ou os modelos treinados (por exemplo, ataques antagónicos), ou explorar vulnerabilidades dos ativos digitais do sistema de IA ou da infraestrutura de tecnologias da informação e comunicação (TIC) subjacente. A fim de assegurar um nível de cibersegurança adequado aos riscos, os fornecedores de sistemas de IA de risco elevado devem tomar medidas adequadas, tendo ainda em devida conta a infraestrutura de TIC subjacente.

(52)No âmbito da legislação de harmonização da União, devem ser estabelecidas regras aplicáveis à colocação no mercado, à colocação em serviço e à utilização de sistemas de IA de risco elevado coerentes com o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho 51 , que estabelece os requisitos de acreditação e fiscalização de produtos, a Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho 52 , relativa a um quadro comum para a comercialização de produtos, e o Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho 53 , relativo à fiscalização do mercado e à conformidade dos produtos (a seguir designados conjuntamente por «novo quadro legislativo [para a comercialização de produtos]»).

(53)É apropriado que uma pessoa singular ou coletiva específica, identificada como «fornecedor», assuma a responsabilidade pela colocação no mercado ou pela colocação em serviço de um sistema de IA de risco elevado, independentemente de ser ou não a pessoa que concebeu ou desenvolveu o sistema.

(54)O fornecedor deve introduzir um sistema de gestão da qualidade sólido, garantir a realização do procedimento de avaliação da conformidade exigido, elaborar a documentação pertinente e estabelecer um sistema de acompanhamento pós-comercialização capaz. As autoridades públicas que colocam em serviço sistemas de IA de risco elevado para sua própria utilização podem adotar e aplicar as regras relativas ao sistema de gestão da qualidade no âmbito do sistema de gestão da qualidade adotado a nível nacional ou regional, consoante o caso, tendo em conta as especificidades do setor e as competências e a organização da autoridade pública em causa.

(55)Caso um sistema de IA de risco elevado que é um componente de segurança de um produto abrangido por legislação setorial do novo quadro legislativo não seja colocado no mercado ou em serviço de forma independente desse produto, o fabricante do produto final, conforme definido no correspondente ato do novo quadro legislativo, deve cumprir as obrigações dos fornecedores estabelecidas no presente regulamento e assegurar que o sistema de IA integrado no produto final cumpre os requisitos do presente regulamento.

(56)Para permitir a execução do presente regulamento e criar condições de concorrência equitativas para os operadores, tendo ainda em conta as diferentes formas de disponibilização de produtos digitais, é importante assegurar que, em qualquer circunstância, uma pessoa estabelecida na União possa fornecer às autoridades todas as informações necessárias sobre a conformidade de um sistema de IA. Como tal, antes de disponibilizarem os seus sistemas de IA na União, caso não seja possível identificar um importador, os fornecedores estabelecidos fora da União devem, através de mandato escrito, designar um mandatário estabelecido na União.

(57)Em consonância com os princípios do novo quadro legislativo, devem ser estabelecidas obrigações específicas aplicáveis a determinados operadores económicos,

como os importadores e os distribuidores, de modo que garanta a segurança jurídica e facilite a conformidade regulamentar desses operadores.

(58)Dada a natureza dos sistemas de IA e os riscos para a segurança e os direitos fundamentais possivelmente associados à sua utilização, nomeadamente no que respeita à necessidade de assegurar um controlo adequado do desempenho de um sistema de IA num cenário real, é apropriado determinar responsabilidades específicas para os utilizadores. Em particular, os utilizadores devem utilizar os sistemas de IA de risco elevado de acordo com as instruções de utilização e devem ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso.

(59)É apropriado definir que o utilizador do sistema de IA é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo sob cuja autoridade o sistema de IA é operado, salvo se o sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional.

(60)Face à complexidade da cadeia de valor da inteligência artificial, determinados terceiros, nomeadamente os envolvidos na venda e no fornecimento de software, ferramentas e componentes de software, modelos pré-treinados e dados, ou os fornecedores de serviços de rede, devem cooperar, consoante o caso, com os fornecedores e os utilizadores, para permitir que estes cumpram as obrigações estabelecidas no presente regulamento, e com as autoridades competentes estabelecidas no presente regulamento.

(61)A normalização deve desempenhar um papel fundamental, disponibilizando aos fornecedores soluções técnicas que assegurem o cumprimento do presente regulamento. O cumprimento de normas harmonizadas, conforme definido no Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho 54 , deve constituir um meio de os fornecedores demonstrarem a conformidade com os requisitos do presente regulamento. Contudo, a Comissão pode adotar especificações técnicas comuns em domínios onde não existem normas harmonizadas ou onde estas são insuficientes.

(62)A fim de assegurar um nível elevado de fiabilidade dos sistemas de IA de risco elevado, estes devem ser sujeitos a uma avaliação da conformidade antes de serem colocados no mercado ou em serviço.

(63)Para minimizar os encargos impostos aos operadores e evitar possíveis duplicações, é apropriado que, no caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos por legislação de harmonização da União na sequência da abordagem do novo quadro legislativo, o cumprimento dos requisitos do presente regulamento por parte desses sistemas de IA seja aferido no âmbito da avaliação da conformidade já prevista nessa legislação. Como tal, a aplicabilidade dos requisitos do presente regulamento não deve afetar a lógica, a metodologia ou a estrutura geral específica da avaliação da conformidade realizada nos termos do correspondente ato do novo quadro legislativo. Esta abordagem encontra-se refletida na íntegra na interligação entre o presente regulamento e o [Regulamento Máquinas]. Embora os riscos de segurança dos sistemas de IA que garantem funções de segurança nas máquinas sejam tratados nos requisitos do presente regulamento, determinados requisitos específicos do [Regulamento Máquinas] assegurarão a integração segura de sistemas de IA nas máquinas em geral, de modo que

não ponha em causa a segurança das máquinas no seu todo. O [Regulamento Máquinas] aplica a mesma definição de sistema de IA do presente regulamento.

(64)Dada a experiência mais vasta dos certificadores de pré-comercialização profissionais no domínio da segurança dos produtos e a diferente natureza dos riscos inerentes, é apropriado limitar, pelo menos numa fase inicial da aplicação do presente regulamento, o âmbito da avaliação da conformidade por terceiros aos sistemas de IA de risco elevado que não estejam relacionados com produtos. Como tal, a avaliação da conformidade desses sistemas deve ser realizada, regra geral, pelo fornecedor sob a sua própria responsabilidade, com a exceção única dos sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, cuja avaliação da conformidade, contanto que os sistemas em causa não sejam proibidos, deve contar com a participação de um organismo notificado.

(65)Para efeitos de avaliação da conformidade por terceiros de sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, o presente regulamento prevê que as autoridades nacionais competentes designem organismos notificados, os quais devem cumprir uma série de requisitos, nomeadamente em termos de independência, competência e ausência de conflitos de interesse.

(66)Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, é apropriado que um sistema de IA seja objeto de uma nova avaliação da conformidade sempre que seja alterado de maneira que possa afetar o cumprimento do presente regulamento ou que a finalidade prevista do sistema se altere. Além disso, no que respeita aos sistemas de IA que continuam a «aprender» depois de terem sido colocados no mercado ou em serviço (ou seja, que adaptam automaticamente o modo de funcionamento), é necessário criar regras que determinem que as alterações do algoritmo e do desempenho predeterminados pelo fornecedor e examinados aquando da avaliação da conformidade não constituem uma modificação substancial.

(67)Para que possam circular livremente dentro do mercado interno, os sistemas de IA de risco elevado devem apresentar a marcação CE para indicar o cumprimento do presente regulamento. Os Estados-Membros não podem criar obstáculos injustificados à colocação no mercado ou à colocação em serviço de sistemas de IA de risco elevado que cumpram os requisitos previstos no presente regulamento e apresentem a marcação CE.

(68)Em certas condições, uma disponibilização rápida de tecnologias inovadoras pode ser crucial para a saúde e a segurança das pessoas e da sociedade em geral. Como tal, é apropriado que, por razões excecionais de segurança pública ou proteção da vida e da saúde das pessoas singulares e de proteção da propriedade industrial e comercial, os Estados-Membros possam autorizar a colocação no mercado ou a colocação em serviço de sistemas de IA que não foram objeto de uma avaliação da conformidade.

(69)Para facilitar o trabalho da Comissão e dos Estados-Membros no domínio da inteligência artificial, bem como aumentar a transparência para o público, os fornecedores de sistemas de IA de risco elevado que não os relacionados com produtos abrangidos pelo âmbito da atual legislação de harmonização da União devem ser obrigados a registar esses sistemas de IA de risco elevado numa base de dados da UE que será criada e gerida pela Comissão. A Comissão deve ser o responsável pelo tratamento dessa base de dados, nos

termos do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho 55 . Para assegurar que a base de dados esteja plenamente operacional à data de implantação, o procedimento para a criação da base de dados deve incluir a elaboração de especificações funcionais pela Comissão e um relatório de auditoria independente.

(70)Determinados sistemas de IA concebidos para interagir com pessoas singulares ou para criar conteúdos podem representar riscos específicos de usurpação de identidade ou fraude, independentemente de serem considerados de risco elevado ou não. Como tal, em certas circunstâncias, a utilização destes sistemas deve ser sujeita a obrigações de transparência específicas sem prejudicar os requisitos e as obrigações aplicáveis aos sistemas de IA de risco elevado. Em particular, as pessoas singulares devem ser notificadas de que estão a interagir com um sistema de IA, a não ser que tal seja óbvio tendo em conta as circunstâncias e o contexto de utilização. Além disso, as pessoas singulares devem ser notificadas quando são expostas a um sistema de reconhecimento de emoções ou a um sistema de categorização biométrica. Essas informações e notificações devem ser fornecidas em formatos acessíveis a pessoas com deficiência. Além disso, os utilizadores que recorrem a um sistema de IA para gerar ou manipular conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, locais ou acontecimentos reais e que, falsamente, pareçam ser autênticos a outrem devem divulgar que os conteúdos foram criados de forma artificial ou manipulados, identificando como tal o resultado da inteligência artificial e divulgando a sua origem artificial.

(71)A inteligência artificial é uma família de tecnologias em rápida evolução que exige novas formas de supervisão regulamentar e um espaço seguro para a experimentação, garantindo ao mesmo tempo uma inovação responsável e a integração de salvaguardas e medidas de atenuação dos riscos adequadas. Para assegurar um quadro jurídico propício à inovação, preparado para o futuro e resistente a perturbações, as autoridades nacionais competentes de um ou vários Estados-Membros devem ser incentivadas a criar ambientes de testagem da regulamentação da inteligência artificial que facilitem o desenvolvimento e o teste de sistemas de IA inovadores sob uma supervisão regulamentar rigorosa, antes que estes sistemas sejam colocados no mercado ou em serviço.

(72)Os objetivos dos ambientes de testagem da regulamentação devem passar por: fomentar a inovação no domínio da IA, mediante a criação de um ambiente controlado de experimentação e teste na fase de desenvolvimento e pré-comercialização, com vista a assegurar que os sistemas de IA inovadores cumprem o presente regulamento e outra legislação aplicável dos Estados-Membros e da União; reforçar a segurança jurídica para os inovadores; melhorar a supervisão e a compreensão, por parte das autoridades competentes, das oportunidades, dos riscos emergentes e dos impactos da utilização da inteligência artificial; e acelerar o acesso aos mercados, nomeadamente por via da eliminação dos entraves para as pequenas e médias empresas (PME) e as empresas em fase de arranque. Para assegurar uma aplicação uniforme em toda a União e economias de escala, é apropriado criar regras comuns para a implantação dos ambientes de testagem da regulamentação e um quadro para a cooperação entre as autoridades competentes envolvidas na supervisão desses ambientes. O presente regulamento deve estabelecer o fundamento jurídico para a utilização de dados pessoais recolhidos para outras finalidades com vista ao desenvolvimento de determinados sistemas de IA por motivos de interesse público no âmbito do ambiente de testagem da regulamentação da IA, em conformidade com o artigo 6.º, n.º 4, do Regulamento (UE) 2016/679 e do artigo 6.º do Regulamento

(UE) 2018/1725 e sem prejuízo do artigo 4.º, n.º 2, da Diretiva (UE) 2016/680. Os participantes no ambiente de testagem devem assegurar salvaguardas adequadas e cooperar com as autoridades competentes, nomeadamente seguindo as suas orientações e atuando de forma célere e de boa-fé para atenuar eventuais riscos elevados para a segurança e os direitos fundamentais que possam revelar-se durante o desenvolvimento e a experimentação no ambiente de testagem. A conduta dos participantes no ambiente de testagem deve ser tida em conta quando as autoridades competentes decidirem sobre a aplicação de uma coima, nos termos do artigo 83.º, n.º 2, do Regulamento (UE) 2016/679 e do artigo 57.º da Diretiva (UE) 2016/680.

(73)A fim de promover e proteger a inovação, é importante ter em especial atenção os interesses dos fornecedores e utilizadores de sistemas de IA de pequena dimensão. Para esse efeito, os Estados-Membros devem desenvolver iniciativas dirigidas a esses operadores, incluindo ações de sensibilização e comunicação de informações. Além disso, os interesses e as necessidades específicas dos fornecedores de pequena dimensão devem ser tidas em conta quando os organismos notificados fixam as taxas a pagar pela avaliação da conformidade. Os custos de tradução associados à documentação obrigatória e à comunicação com as autoridades podem constituir um custo substancial para os fornecedores e outros operadores, nomeadamente para os fornecedores de menor dimensão. Os Estados-Membros podem eventualmente assegurar que uma das línguas por si determinadas e aceites para a elaboração de documentação pelos fornecedores e a comunicação com os operadores seja uma língua amplamente compreendida pelo maior número possível de utilizadores transfronteiras.

(74)Para minimizar os riscos para a aplicação resultantes da falta de conhecimentos e competências especializadas no mercado, bem como facilitar o cumprimento, por parte dos fornecedores e dos organismos notificados, das obrigações que lhes são impostas pelo presente regulamento, a «plataforma IA a pedido», os polos europeus de inovação digital e as instalações de ensaio e experimentação criadas pela Comissão e pelos Estados-Membros a nível nacional ou europeu podem eventualmente contribuir para a aplicação do presente regulamento. No âmbito da respetiva missão e domínios de competência, estas entidades podem prestar apoio técnico e científico aos fornecedores e aos organismos notificados.

(75)É apropriado que a Comissão facilite, tanto quanto possível, o acesso a instalações de teste e experimentação aos organismos, grupos ou laboratórios criados ou acreditados nos termos da legislação de harmonização da União pertinente e que desempenham funções no contexto da avaliação da conformidade dos produtos ou dispositivos abrangidos por essa legislação de harmonização da União. Tal é, nomeadamente, o caso dos painéis de peritos, dos laboratórios especializados e dos laboratórios de referência no domínio dos dispositivos médicos, referidos nos Regulamentos (UE) 2017/745 e (UE) 2017/746.

(76)A fim de facilitar uma aplicação simples, eficaz e harmoniosa do presente regulamento, deve ser criado um Comité Europeu para a Inteligência Artificial. O Comité deve ser responsável por uma série de funções consultivas, nomeadamente a emissão de pareceres, recomendações, conselhos ou orientações em questões relacionadas com a aplicação do presente regulamento, incluindo no tocante a especificações técnicas ou normas existentes relativas aos requisitos indicados no presente regulamento, e a prestação de aconselhamento e assistência à Comissão sobre questões específicas relacionadas com a inteligência artificial.

(77)Os Estados-Membros desempenham um papel fundamental na aplicação e execução do presente regulamento. Nesse sentido, cada Estado-Membro deve designar uma ou várias autoridades nacionais competentes para efeitos de supervisão da aplicação e execução do presente regulamento. A fim de aumentar a eficácia organizativa dos Estados-Membros e de criar um ponto de contacto oficial para o público e outras contrapartes a nível dos Estados-Membros e da União, cada Estado-Membro deve designar uma autoridade nacional como autoridade nacional de controlo.

(78)Para assegurar que os fornecedores de sistemas de IA de risco elevado possam aproveitar a experiência adquirida na utilização de sistemas de IA de risco elevado para melhorarem os seus sistemas e o processo de conceção e desenvolvimento ou possam adotar possíveis medidas corretivas em tempo útil, todos os fornecedores devem dispor de um sistema de acompanhamento pós-comercialização. Este sistema também é fundamental para assegurar uma resolução mais eficaz e atempada dos eventuais riscos decorrentes dos sistemas de IA que continuam a «aprender» depois de terem sido colocados no mercado ou em serviço. Neste contexto, os fornecedores devem ainda ser obrigados a introduzir um sistema para comunicar às autoridades competentes quaisquer incidentes graves ou violações do direito nacional e da União que protege os direitos fundamentais resultantes da utilização dos sistemas de IA que fornecem.

(79)Para assegurar uma execução adequada e eficaz dos requisitos e das obrigações estabelecidas no presente regulamento, que faz parte da legislação de harmonização da União, o sistema de fiscalização do mercado e de conformidade dos produtos estabelecido no Regulamento (UE) 2019/1020 deve ser aplicado na íntegra. Quando tal for necessário ao cumprimento do seu mandato, as autoridades públicas ou os organismos nacionais que supervisionam a aplicação do direito da União que protege direitos fundamentais, incluindo os organismos de promoção da igualdade, também devem ter acesso à documentação elaborada por força do presente regulamento.

(80)A legislação da União em matéria de serviços financeiros inclui regras e requisitos relativos à governação interna e à gestão dos riscos aplicáveis às instituições financeiras regulamentadas durante a prestação desses serviços, incluindo quando estas utilizam sistemas de IA. Para assegurar a coerência na aplicação e na execução das obrigações previstas no presente regulamento e das regras e requisitos da legislação da União aplicáveis aos serviços financeiros, as autoridades responsáveis pela supervisão e execução da legislação no domínio dos serviços financeiros, incluindo, se for caso disso, o Banco Central Europeu, devem ser designadas autoridades competentes para efeitos de supervisão da aplicação do presente regulamento, incluindo o exercício de funções de fiscalização do mercado, no que diz respeito aos sistemas de IA fornecidos ou utilizados por instituições financeiras regulamentadas e supervisionadas. A fim de reforçar a coerência entre o presente regulamento e as regras aplicáveis às instituições de crédito regulamentadas pela Diretiva 2013/36/UE do Parlamento Europeu e do Conselho 56 , também é apropriado integrar o procedimento de avaliação da conformidade e algumas das obrigações processuais dos fornecedores relativas à gestão de riscos, ao acompanhamento pós-comercialização e à documentação nas obrigações e procedimentos em vigor por força da mesma diretiva. No intuito de evitar sobreposições, também devem ser previstas derrogações limitadas no respeitante ao sistema de gestão da qualidade dos fornecedores e à obrigação de controlo imposta aos utilizadores de sistemas de IA de risco

elevado, contanto que tal se aplique a instituições de crédito regulamentadas pela Diretiva 2013/36/UE.

(81)O desenvolvimento de outros sistemas de IA, que não sejam sistemas de IA de risco elevado, de acordo com os requisitos do presente regulamento pode conduzir a uma maior utilização de inteligência artificial fiável na União. Os fornecedores de sistemas de IA que não são de risco elevado devem ser incentivados a criar códigos de conduta que visem promover a aplicação voluntária dos requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado. Os fornecedores devem ainda ser incentivados a aplicar voluntariamente requisitos adicionais relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento. A Comissão pode desenvolver iniciativas, incluindo de natureza setorial, para facilitar a redução de obstáculos técnicos que impeçam o intercâmbio transfronteiras de dados para o desenvolvimento da inteligência artificial, incluindo em matéria de infraestruturas de acesso aos dados e de interoperabilidade semântica e técnica de diferentes tipos de dados.

(82)Não obstante, é importante que os sistemas de IA relacionados com produtos que não são de risco elevado, nos termos do presente regulamento, e que, como tal, não são obrigados a cumprir os requisitos do mesmo, sejam seguros quando são colocados no mercado ou em serviço. A fim de contribuir para alcançar esse objetivo, a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho 57 será aplicada como uma rede de segurança.

(83)Para assegurar uma cooperação de confiança e construtiva entre as autoridades competentes a nível da União e nacional, todas as partes envolvidas na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções.

(84)Os Estados-Membros devem tomar todas as medidas necessárias para assegurar a aplicação das disposições do presente regulamento, inclusive estabelecendo sanções efetivas, proporcionadas e dissuasivas aplicáveis à sua violação. No caso de determinadas violações específicas, os Estados-Membros devem ter em conta as margens e os critérios estabelecidos no presente regulamento. A Autoridade Europeia para a Proteção de Dados deve ter competências para impor coimas às instituições, órgãos e organismos da União que se enquadram no âmbito do presente regulamento.

(85)Para assegurar que é possível adaptar o quadro regulamentar quando necessário, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão no que diz respeito à alteração das técnicas e abordagens que definem sistemas de IA mencionadas no anexo I, da legislação de harmonização da União enumerada no anexo II, da lista de sistemas de IA de risco elevado constante do anexo III, das disposições relativas à documentação técnica que constam do anexo IV, do conteúdo da declaração de conformidade UE estabelecido no anexo V, das disposições relativas aos procedimentos de avaliação da conformidade que constam dos anexos VI e VII e das disposições que definem os sistemas de IA de risco elevado aos quais se deve aplicar o procedimento de avaliação da conformidade com base na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive

ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor 58 . Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(86)A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho 59 .

(87)Atendendo a que o objetivo do presente regulamento não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão ou aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

(88)O presente regulamento deve aplicar-se a partir de … [Serviço das Publicações: inserir a data estabelecida no artigo 85.º]. Contudo, as estruturas relacionadas com a governação e o sistema de avaliação da conformidade devem estar operacionais antes dessa data, pelo que as disposições relativas aos organismos notificados e à estrutura de governação devem aplicar-se a partir de … [Serviço das Publicações: inserir a data correspondente a três meses a contar da data de entrada em vigor do presente regulamento]. Além disso, os Estados-Membros devem estabelecer as regras em matéria de sanções, incluindo coimas, e notificá-las à Comissão, bem como assegurar que sejam aplicadas de forma efetiva e adequada à data de aplicação do presente regulamento. Como tal, as disposições relativas às sanções devem aplicar-se a partir de … [Serviço das Publicações: inserir a data correspondente a doze meses a contar da data de entrada em vigor do presente regulamento].

(89)A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados foram consultados nos termos do artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725, e emitiram parecer em […],

ADOTARAM O PRESENTE REGULAMENTO:

TÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento estabelece:

a)Regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial («sistemas de IA») na União;

b)Proibições de certas práticas de inteligência artificial;

c)Requisitos específicos para sistemas de IA de risco elevado e obrigações para os operadores desses sistemas;

d)Regras de transparência harmonizadas para sistemas de IA concebidos para interagir com pessoas singulares, sistemas de reconhecimento de emoções e sistemas de categorização biométrica, bem como para sistemas de IA usados para gerar ou manipular conteúdos de imagem, áudio ou vídeo;

e)Regras relativas à fiscalização e vigilância do mercado.

Artigo 2.º

Âmbito

1.O presente regulamento é aplicável a:

a)Fornecedores que coloquem no mercado ou coloquem em serviço sistemas de IA no território da União, independentemente de estarem estabelecidos na União ou num país terceiro;

b)Utilizadores de sistemas de IA localizados na União;

c)Fornecedores e utilizadores de sistemas de IA localizados num país terceiro, se o resultado produzido pelo sistema for utilizado na União.

2.Aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo âmbito dos atos a seguir enumerados, apenas é aplicável o artigo 84.º do presente regulamento:

a)Regulamento (CE) n.º 300/2008;

b)Regulamento (UE) n.º 167/2013;

c)Regulamento (UE) n.º 168/2013;

d)Diretiva 2014/90/UE;

e)Diretiva (UE) 2016/797;

f)Regulamento (UE) 2018/858;

g)Regulamento (UE) 2018/1139;

h)Regulamento (UE) 2019/2144.

3.O presente regulamento não se aplica aos sistemas de IA desenvolvidos ou usados exclusivamente para fins militares.

4.O presente regulamento não se aplica a autoridades públicas de países terceiros, nem a organizações internacionais abrangidas pelo âmbito do presente regulamento nos termos do n.º 1, quando essas autoridades ou organizações usem sistemas de IA no âmbito de acordos internacionais para efeitos de cooperação policial e judiciária com a União ou com um ou vários Estados-Membros.

5.O presente regulamento não afeta a aplicação das disposições relativas à responsabilidade dos prestadores intermediários de serviços estabelecidas no capítulo II, secção IV, da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho 60 [a substituir pelas disposições correspondentes do Regulamento Serviços Digitais].

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1)«Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões,

recomendações ou decisões, que influenciam os ambientes com os quais interage;
2)«Fornecedor», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido com vista à sua colocação no mercado ou colocação em serviço sob o seu próprio nome ou marca, a título oneroso ou gratuito;
3)«Fornecedor de pequena dimensão», um fornecedor que seja uma micro ou pequena empresa na aceção da Recomendação 2003/361/CE da Comissão 61 ;
4)«Utilizador», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional;
5)«Mandatário», uma pessoa singular ou coletiva estabelecida na União que tenha recebido um mandato escrito de um fornecedor de um sistema de IA para, respetivamente, executar e cumprir em seu nome as obrigações e os procedimentos previstos no presente regulamento;
6)«Importador», uma pessoa singular ou coletiva estabelecida na União que coloca no mercado ou coloca em serviço um sistema de IA que ostenta o nome ou a marca de uma pessoa singular ou coletiva estabelecida fora da União;
7)«Distribuidor», uma pessoa singular ou coletiva inserida na cadeia de abastecimento, distinta do fornecedor e do importador, que disponibiliza um sistema de IA no mercado da União sem alterar as suas propriedades;
8)«Operador», um fornecedor, utilizador, mandatário, importador ou distribuidor;
9)«Colocação no mercado», a primeira disponibilização de um sistema de IA no mercado da União;
10)«Disponibilização no mercado», o fornecimento de um sistema de IA para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial, a título oneroso ou gratuito;
11)«Colocação em serviço», o fornecimento de um sistema de IA para a primeira utilização no mercado da União, diretamente ao utilizador ou para utilização própria, para a finalidade prevista;
12)«Finalidade prevista», a utilização à qual o fornecedor destina o sistema de IA, incluindo o contexto específico e as condições de utilização, conforme especificado nas informações facultadas pelo fornecedor nas instruções de utilização, nos materiais e declarações promocionais ou de venda, bem como na documentação técnica;
13)«Utilização indevida razoavelmente previsível», a utilização de um sistema de IA de uma forma não conforme com a sua finalidade prevista, mas que pode resultar de comportamentos humanos ou de interações com outros sistemas razoavelmente previsíveis;
14)«Componente de segurança de um produto ou sistema», um componente de um produto ou sistema que cumpre uma função de segurança nesse produto ou sistema ou cuja falha ou anomalia põe em risco a segurança e a saúde de pessoas ou bens;
15)«Instruções de utilização», as informações facultadas pelo fornecedor para esclarecer o utilizador, em especial, sobre a finalidade prevista e a utilização correta de um sistema de IA, incluindo o enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado;

16)«Recolha de um sistema de IA», qualquer medida que vise obter a devolução ao fornecedor de um sistema de IA disponibilizado a utilizadores;
17)«Retirada de um sistema de IA», qualquer medida que vise impedir a distribuição, apresentação ou oferta de um sistema de IA;
18)«Desempenho de um sistema de IA», a capacidade de um sistema de IA para alcançar a sua finalidade prevista;
19)«Autoridade notificadora», a autoridade nacional responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação de organismos de avaliação da conformidade e pela fiscalização destes;
20)«Avaliação da conformidade», o processo de verificar se estão preenchidos os requisitos estabelecidos no título III, capítulo 2, do presente regulamento relacionados com um sistema de IA;
21)«Organismo de avaliação da conformidade», um organismo que realiza atividades de avaliação da conformidade por terceiros, nomeadamente testagem, certificação e inspeção;
22)«Organismo notificado», um organismo de avaliação da conformidade designado nos termos do presente regulamento ou de outra legislação de harmonização da União aplicável;
23)«Modificação substancial», uma alteração do sistema de IA após a sua colocação no mercado ou colocação em serviço que afeta a conformidade do sistema de IA com os requisitos estabelecidos no título III, capítulo 2, do presente regulamento ou conduz a uma modificação da finalidade prevista relativamente à qual o sistema de IA foi avaliado;
24)«Marcação de conformidade CE» (marcação CE), a marcação pela qual um fornecedor atesta que um sistema de IA está em conformidade com os requisitos estabelecidos no título III, capítulo 2, do presente regulamento e na restante legislação da União aplicável que harmoniza as condições de comercialização de produtos («legislação de harmonização da União») em que seja prevista a respetiva aposição;
25)«Acompanhamento pós-comercialização», todas as atividades que os fornecedores de sistemas de IA empreendem para recolher e analisar proativamente dados sobre a experiência adquirida com a utilização de sistemas de IA que colocaram no mercado ou em serviço, com vista a identificar a eventual necessidade de aplicar imediatamente quaisquer medidas corretivas ou preventivas necessárias;
26)«Autoridade de fiscalização do mercado», a autoridade nacional que realiza as atividades e toma medidas nos previstas no Regulamento (UE) 2019/1020;
27)«Norma harmonizada», uma norma europeia, na aceção do artigo 2.º, n.º 1, alínea c), do Regulamento (UE) n.º 1025/2012;
28)«Especificações comuns», um documento, que não uma norma, que contém soluções técnicas que proporcionam um meio para cumprir certos requisitos e obrigações estabelecidas no presente regulamento;
29)«Dados de treino», os dados usados para treinar um sistema de IA mediante o ajustamento dos seus parâmetros passíveis de serem aprendidos, incluindo os pesos de uma rede neuronal;
30)«Dados de validação», os dados utilizados para realizar uma avaliação do sistema de IA treinado e para ajustar os seus parâmetros não passíveis de serem aprendidos e o seu processo de aprendizagem, a fim de, entre outros objetivos, evitar um sobreajustamento; sendo que o conjunto de dados de validação pode

ser um conjunto de dados separado ou parte de um conjunto de dados de treino, quer como divisão fixa ou variável;
31)«Dados de teste», os dados utilizados para realizar uma avaliação independente do sistema de IA treinado e validado, a fim de confirmar o desempenho esperado desse sistema antes de ser colocado no mercado ou em serviço;
32)«Dados de entrada», os dados fornecidos a um sistema de IA, ou por ele obtidos diretamente, com base nos quais o sistema produz um resultado;
33)«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico das características físicas, fisiológicas ou comportamentais de uma pessoa singular, os quais permitem obter ou confirmar a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;
34)«Sistema de reconhecimento de emoções», um sistema de IA concebido para identificar ou inferir emoções ou intenções de pessoas singulares com base nos seus dados biométricos;
35)«Sistema de categorização biométrica», um sistema de IA concebido para classificar pessoas singulares em categorias específicas, tais como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, origem étnica ou orientação sexual ou política, com base nos seus dados biométricos;
36)«Sistema de identificação biométrica à distância», um sistema de IA concebido para identificar pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que o utilizador do sistema de IA saiba antecipadamente se a pessoa em causa estará presente e pode ser identificada;
37)«Sistema de identificação biométrica à distância "em tempo real"», um sistema de identificação biométrica à distância em que a recolha de dados biométricos, a comparação e a identificação ocorrem sem atraso significativo. Para evitar que as regras sejam contornadas, tal inclui não apenas a identificação instantânea, mas também a identificação com ligeiro atraso;
38)«Sistema de identificação biométrica à distância "em diferido"», um sistema de identificação biométrica à distância que não seja um sistema de identificação biométrica à distância em «tempo real»;
39)«Espaço acessível ao público», qualquer espaço físico aberto ao público, independentemente da eventual aplicação de condições de acesso específicas;
40)«Autoridade policial»:

a)Uma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas; ou

b)Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer autoridade pública e poderes públicos para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

41)«Manutenção da ordem pública», as atividades realizadas por autoridades policiais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

42)«Autoridade nacional de controlo», a autoridade à qual um Estado-Membro atribui a responsabilidade pela execução e aplicação do presente regulamento, pela coordenação das atividades confiadas a esse Estado-Membro, por atuar como ponto de contacto único para a Comissão e por representar o Estado-Membro no Comité Europeu para a Inteligência Artificial;

43)«Autoridade nacional competente», a autoridade de controlo, a autoridade notificadora ou a autoridade de fiscalização do mercado designadas a nível nacional;

44)«Incidente grave», qualquer incidente que, direta ou indiretamente, tenha, poderia ter tido ou possa vir a ter alguma das seguintes consequências:

a)A morte de uma pessoa ou danos graves para a saúde de uma pessoa, bens, ou o ambiente,

b)Uma perturbação grave e irreversível da gestão e do funcionamento de uma infraestrutura crítica.

Artigo 4.º

Alterações do anexo I

A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar a lista de técnicas e abordagens enumeradas no anexo I, a fim de a atualizar face à evolução do mercado e da tecnologia com base em características similares às técnicas e abordagens constantes da lista.

TÍTULO II
PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS

Artigo 5.º

1.Estão proibidas as seguintes práticas de inteligência artificial:

a)A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que empregue técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

b)A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade ou deficiência física ou mental, a fim de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

c)A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA por autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a uma das seguintes situações ou a ambas:

i)tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos,

ii)tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é injustificado e desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

d)A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos:

i)a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas,

ii)a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista,

iii)a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho 62 e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro.

2.A utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve ter em conta os seguintes elementos:

a)A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema;

b)As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas.

3.No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização específica de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização e esta pode ser solicitada apenas durante ou após a utilização.

A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância «em tempo real» em apreço é necessária e proporcionada para alcançar um dos objetivos

especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2.

4.Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n.os 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública.

TÍTULO III
SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO
CAPÍTULO 1
CLASSIFICAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL COMO SENDO DE RISCO ELEVADO

Artigo 6.º

Regras para a classificação de sistemas de inteligência artificial de risco elevado

1.Independentemente de a colocação no mercado ou a colocação em serviço de um sistema de IA ser feita separadamente dos produtos a que se referem as alíneas a) e b), esse sistema de IA é considerado de risco elevado quando estejam satisfeitas ambas as condições que se seguem:

a)O sistema de IA destina-se a ser utilizado como um componente de segurança de um produto ou é, ele próprio, um produto abrangido pela legislação de harmonização da União enumerada no anexo II;

b)Nos termos da legislação de harmonização da União enumerada no anexo II, o produto cujo componente de segurança é o sistema de IA, ou o próprio sistema de IA enquanto produto deve ser sujeito a uma avaliação da conformidade por terceiros com vista à colocação no mercado ou à colocação em serviço.

2.Além dos sistemas de IA de risco elevado referidos no n.º 1, os sistemas de IA referidos no anexo III são também considerados de risco elevado.

Artigo 7.º

Alterações do anexo III

1.A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar a lista do anexo III, aditando sistemas de IA de risco elevado que preencham ambas as condições que se seguem:

a)Os sistemas de IA destinam-se a ser utilizados em qualquer um dos domínios enumerados no anexo III, pontos 1 a 8;

b)Os sistemas de IA representam um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais que, em termos de gravidade e probabilidade de ocorrência, é equivalente ou superior ao risco de danos ou impacto adverso representado pelos sistemas de IA de risco elevado já referidos no anexo III.

2.Ao avaliar, para efeitos do disposto no n.º 1, se um sistema de IA representa um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais equivalente ou superior ao risco de danos representado pelos sistemas de IA de risco elevado já referidos no anexo III, a Comissão tem em consideração os seguintes critérios:

a)A finalidade prevista do sistema de IA;

b)O grau de utilização efetiva ou a probabilidade de utilização de um sistema de IA;

c)Em que medida a utilização de um sistema de IA já causou danos para a saúde e a segurança ou um impacto adverso nos direitos fundamentais ou suscitou preocupações significativas quanto à concretização desses danos ou desse impacto adverso, conforme demonstrado por relatórios ou alegações documentadas apresentadas às autoridades nacionais competentes;

d)O potencial grau desses danos ou desse impacto adverso, nomeadamente em termos de intensidade e de capacidade para afetar um grande número de pessoas;

e)O grau de dependência das pessoas potencialmente lesadas ou adversamente afetadas em relação ao resultado produzido por um sistema de IA, em especial se, por razões práticas ou jurídicas, aquelas não puderem razoavelmente autoexcluir-se desse resultado;

f)A posição de vulnerabilidade das pessoas potencialmente prejudicadas ou adversamente afetadas em relação ao utilizador de um sistema de IA, nomeadamente devido a um desequilíbrio de poder ou de conhecimento, a circunstâncias económicas ou sociais, ou à idade;

g)A facilidade de reversão do resultado produzido com um sistema de IA, tendo em conta que os resultados com impacto na saúde ou na segurança das pessoas não podem ser considerados como facilmente reversíveis;

h)Em que medida a legislação da União em vigor prevê:

i)medidas de reparação eficazes em relação aos riscos representados por um sistema de IA, com exclusão de pedidos de indemnização,

ii)medidas eficazes para prevenir ou minimizar substancialmente esses riscos.

CAPÍTULO 2
REQUISITOS APLICÁVEIS A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

Artigo 8.º
Cumprimento dos requisitos

1.Os sistemas de IA de risco elevado devem cumprir os requisitos estabelecidos neste capítulo.

2.A finalidade prevista do sistema de IA de risco elevado e o sistema de gestão de riscos a que se refere o artigo 9.º devem ser tidos em conta para efeitos do cumprimento desses requisitos.

Artigo 9.º
Sistema de gestão de riscos

1.Deve ser criado, implantado, documentado e mantido um sistema de gestão de riscos em relação a sistemas de IA de risco elevado.

2.O sistema de gestão de riscos deve consistir num processo iterativo contínuo, executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado,

o que requer atualizações regulares sistemáticas. Deve compreender as seguintes etapas:

a)Identificação e análise dos riscos conhecidos e previsíveis associados a cada sistema de IA de risco elevado;

b)Estimativa e avaliação de riscos que podem surgir quando o sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista e em condições de utilização indevida razoavelmente previsíveis;

c)Avaliação de outros riscos que possam surgir, baseada na análise dos dados recolhidos a partir do sistema de acompanhamento pós-comercialização a que se refere o artigo 61.º;

d)Adoção de medidas de gestão de riscos adequadas em conformidade com o disposto nos números que se seguem.

3.As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem ter em devida consideração os efeitos e eventuais interações resultantes da aplicação combinada dos requisitos estabelecidos no presente capítulo. Devem também ter em conta o estado da técnica geralmente reconhecido, incluindo o que se encontrar refletido em normas harmonizadas ou especificações comuns pertinentes.

4.As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem levar a que o eventual risco residual associado a cada perigo, bem como o risco residual global dos sistemas de IA de risco elevado, sejam considerados aceitáveis, contanto que o sistema de IA de risco elevado seja usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis. Os riscos residuais devem ser comunicados ao utilizador.

Ao identificar as medidas de gestão de riscos mais apropriadas, deve assegurar-se o seguinte:

a)Eliminação ou redução de riscos tanto quanto possível, graças a processos de conceção e desenvolvimento adequados;

b)Se for caso disso, adoção de medidas de atenuação e controlo adequadas em relação a riscos que não possam ser eliminados;

c)Prestação de informações adequadas nos termos do artigo 13.º, em especial no atinente aos riscos a que se refere o n.º 2, alínea b), do presente artigo e, se for caso disso, formação dos utilizadores.

Na eliminação ou redução de riscos relacionados com a utilização do sistema de IA de risco elevado, há que ter em consideração o conhecimento técnico, a experiência, a educação e a formação que se pode esperar que o utilizador possua e o ambiente em que está previsto utilizar o sistema.

5.Os sistemas de IA de risco elevado devem ser sujeitos a testes para que se identifiquem as medidas de gestão de riscos mais apropriadas. Os testes asseguram que os sistemas de IA de risco elevado tenham um desempenho coerente com a finalidade prevista e que cumpram os requisitos estabelecidos no presente capítulo.

6.Os procedimentos de teste são adequados para alcançar a finalidade prevista do sistema de IA e não precisam de ir além do necessário para alcançar essa finalidade.

7.Os testes dos sistemas de IA de risco elevado devem ser realizados, consoante apropriado, em qualquer momento durante o processo de desenvolvimento e, em qualquer caso, antes da colocação no mercado ou da colocação em serviço. Os testes devem ser realizados relativamente a métricas previamente definidas e a

limiares probabilísticos que são apropriados para a finalidade prevista do sistema de IA de risco elevado.
8.Ao implantar o sistema de gestão de riscos descrito nos n.os 1 a 7, deve tomar-se especificamente em conta se o sistema de IA de risco elevado é suscetível de ser acedido por crianças ou de ter impacto nas mesmas.
9.Em relação às instituições de crédito regulamentadas pela Diretiva 2013/36/UE, os aspetos descritos nos n.os 1 a 8 fazem parte dos procedimentos de gestão de riscos estabelecidos por essas instituições nos termos do artigo 74.º da referida diretiva.

Artigo 10.º
Dados e governação de dados

1.Os sistemas de IA de risco elevado que utilizem técnicas que envolvam o treino de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de treino, validação e teste que cumpram os critérios de qualidade referidos nos n.os 2 a 5.
2.Os conjuntos de dados de treino, validação e teste devem estar sujeitos a práticas adequadas de governação e gestão de dados. Essas práticas dizem nomeadamente respeito:

a)Às escolhas de conceção tomadas;
b)À recolha de dados;
c)Às operações de preparação e tratamento de dados necessárias, tais como anotação, rotulagem, limpeza, enriquecimento e agregação;
d)À formulação dos pressupostos aplicáveis, nomeadamente no que diz respeito às informações que os dados devem medir e representar;
e)À avaliação prévia da disponibilidade, quantidade e adequação dos conjuntos de dados que são necessários;
f)Ao exame para detetar eventuais enviesamentos;
g)À identificação de eventuais lacunas ou deficiências de dados e de possíveis soluções para as mesmas.

3.Os conjuntos de dados de treino, validação e teste devem ser pertinentes, representativos, isentos de erros e completos. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em que o sistema de IA de risco elevado se destina a ser utilizado. Estas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.
4.Os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado.
5.Na medida do estritamente necessário para assegurar o controlo, a deteção e a correção de enviesamentos em relação a sistemas de IA de risco elevado, os fornecedores desses sistemas podem tratar categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, o artigo 10.º da Diretiva (UE) 2016/680 e o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725, assegurando salvaguardas adequadas dos direitos fundamentais e liberdades das pessoas singulares, incluindo impor limitações técnicas à reutilização e utilizar medidas de segurança e preservação da privacidade de

última geração, tais como a pseudonimização ou a cifragem nos casos em que a anonimização possa afetar significativamente a finalidade preconizada.
6.Devem ser aplicadas práticas adequadas de governação e gestão de dados ao desenvolvimento de sistemas de IA de risco elevado que não utilizam técnicas que envolvem o treino de modelos, para assegurar que esses sistemas de IA de risco elevado cumprem o disposto no n.º 2.

Artigo 11.º
Documentação técnica

1.A documentação técnica de um sistema de IA de risco elevado deve ser elaborada antes da colocação no mercado ou colocação em serviço desse sistema e mantida atualizada.
A documentação técnica deve ser elaborada de maneira que demonstre que o sistema de IA de risco elevado cumpre os requisitos estabelecidos no presente capítulo e deve facultar às autoridades nacionais competentes e aos organismos notificados todas as informações necessárias para aferir a conformidade do sistema de IA com esses requisitos. A documentação técnica deve conter, no mínimo, os elementos previstos no anexo IV.
2.Caso um sistema de IA de risco elevado relacionado com um produto, ao qual sejam aplicáveis os atos jurídicos enumerados no anexo II, secção A, seja colocado no mercado ou colocado em serviço, deve ser elaborada uma única documentação técnica que contenha todas as informações enumeradas no anexo IV e as informações exigidas nos termos desses atos jurídicos.
3.A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar o anexo IV, se for caso disso, com vista a assegurar que, tendo em conta a evolução técnica, a documentação técnica forneça todas as informações necessárias para aferir a conformidade do sistema com os requisitos estabelecidos no presente capítulo.

Artigo 12.º
Manutenção de registos

1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos com capacidades que permitam o registo automático de eventos («registos») enquanto o sistema de IA de risco elevado estiver em funcionamento. Essas capacidades de registo devem estar em conformidade com normas reconhecidas ou especificações comuns.
2.As capacidades de registo devem assegurar um nível de rastreabilidade do funcionamento do sistema de IA ao longo do seu ciclo de vida que seja adequado à finalidade prevista do sistema.
3.Em especial, as capacidades de registo devem permitir o controlo do funcionamento do sistema de IA de risco elevado no que diz respeito à ocorrência de situações que possam dar azo a que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, ou dar origem a uma modificação substancial, e facilitar o acompanhamento pós-comercialização a que se refere o artigo 61.º.
4.Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as capacidades de registo devem proporcionar, no mínimo:

a)O registo do período de cada utilização do sistema (data e hora de início e data e hora de fim de cada utilização);

b)A base de dados de referência relativamente à qual os dados de entrada foram verificados pelo sistema;
c)Os dados de entrada cuja pesquisa conduziu a uma correspondência;
d)A identificação das pessoas singulares envolvidas na verificação dos resultados, conforme referido no artigo 14.º, n.º 5.

Artigo 13.º
Transparência e prestação de informações aos utilizadores

1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente para permitir aos utilizadores interpretar o resultado do sistema e utilizá-lo corretamente. Deve ser garantido um tipo e um grau adequado de transparência, que permita cumprir as obrigações que incumbem ao utilizador e ao fornecedor por força do capítulo 3 do presente título.
2.Os sistemas de IA de risco elevado devem ser acompanhados de instruções de utilização, num formato digital ou outro adequado, que incluam informações concisas, completas, corretas e claras que sejam pertinentes, acessíveis e compreensíveis para os utilizadores.
3.As informações a que se refere o n.º 2 devem especificar:
a)A identidade e os dados de contacto do fornecedor e, se for caso disso, do seu mandatário;
b)As características, capacidades e limitações de desempenho do sistema de IA de risco elevado, incluindo:
i)a finalidade prevista do sistema,
ii)o nível de exatidão, solidez e cibersegurança a que se refere o artigo 15.º relativamente ao qual o sistema de IA de risco elevado foi testado e validado e que pode ser esperado, bem como quaisquer circunstâncias conhecidas e previsíveis que possam ter um impacto nesse nível esperado de exatidão, solidez e cibersegurança,
iii)qualquer circunstância conhecida ou previsível, relacionada com a utilização do sistema de IA de risco elevado de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, que possa causar riscos para a saúde e a segurança ou os direitos fundamentais,
iv)o desempenho do sistema no tocante às pessoas ou grupos de pessoas em que o sistema se destina a ser utilizado,
v)quando oportuno, especificações para os dados de entrada, ou quaisquer outras informações importantes em termos dos conjuntos de dados de treino, validação e teste usados, tendo em conta a finalidade prevista do sistema de IA;
c)As alterações do sistema de IA de risco elevado e do seu desempenho que foram predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial, se for caso disso;
d)As medidas de supervisão humana a que se refere o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores;
e)A vida útil esperada do sistema de IA de risco elevado e quaisquer medidas de manutenção e assistência necessárias para assegurar o correto funcionamento desse sistema de IA, incluindo no tocante a atualizações do software.

Artigo 14.º
Supervisão humana

1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA.

2.A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos neste capítulo.

3.A supervisão humana deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas:

a)Medidas identificadas e integradas, quando tecnicamente viável, pelo fornecedor no sistema de IA de risco elevado antes de este ser colocado no mercado ou colocado em serviço;

b)Medidas identificadas pelo fornecedor antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que sejam adequadas para implantação por parte do utilizador.

4.As medidas a que se refere o n.º 3 devem permitir que as pessoas responsáveis pela supervisão humana façam o seguinte, em função das circunstâncias:

a)Compreendam completamente as capacidades e limitações do sistema de IA de risco elevado e sejam capazes de controlar devidamente o seu funcionamento, de modo que os sinais de anomalias, disfuncionalidades e desempenho inesperado possam ser detetados e resolvidos o mais rapidamente possível;

b)Estejam conscientes da possível tendência para confiar automaticamente ou confiar excessivamente no resultado produzido pelo sistema de IA de risco elevado («enviesamento da automatização»), em especial relativamente aos sistemas de IA de risco elevado usados para fornecer informações ou recomendações com vista à tomada de decisões por pessoas singulares;

c)Sejam capazes de interpretar corretamente o resultado do sistema de IA de risco elevado, tendo em conta, nomeadamente, as características do sistema e as ferramentas e os métodos de interpretação disponíveis;

d)Sejam capazes de decidir, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter o resultado do sistema de IA de risco elevado;

e)Serem capazes de intervir no funcionamento do sistema de IA de risco elevado ou interromper o sistema por meio de um botão de «paragem» ou procedimento similar.

5.Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as medidas referidas no n.º 3 devem, além disso, permitir assegurar que nenhuma ação ou decisão seja tomada pelo utilizador com base na identificação resultante do sistema, salvo se a mesma tiver sido verificada e confirmada por, pelo menos, duas pessoas singulares.

Artigo 15.º

Exatidão, solidez e cibersegurança

1.Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o ciclo de vida.

2.As instruções de utilização que acompanham os sistemas de IA de risco elevado devem declarar os níveis de exatidão e a métrica de exatidão aplicável.

3.Os sistemas de IA de risco elevado devem ser resistentes a erros, falhas ou incoerências que possam ocorrer no sistema ou no ambiente em que aquele opera, em especial devido à interação com pessoas singulares ou outros sistemas.

A solidez dos sistemas de IA de risco elevado pode ser alcançada por via de soluções de redundância técnica, que podem incluir planos de reserva ou de segurança à prova de falhas.

Os sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço devem ser desenvolvidos de maneira que assegure que os resultados possivelmente enviesados devido a resultados usados como dados de entrada para futuras operações («circuitos de realimentação») sejam devidamente abordados por via de medidas de atenuação adequadas.

4.Os sistemas de IA de risco elevado devem ser resistentes a tentativas de terceiros não autorizados de alterar a sua utilização ou desempenho explorando as vulnerabilidades do sistema.

As soluções técnicas destinadas a assegurar a cibersegurança dos sistemas de IA de risco elevado devem ser adequadas às circunstâncias e aos riscos de cada caso.

As soluções técnicas para resolver vulnerabilidades específicas da inteligência artificial devem incluir, se for caso disso, medidas para prevenir e controlar ataques que visem manipular o conjunto de dados de treino («contaminação de dados»), dados de entrada preparados para fazer com que o modelo cometa um erro («exemplos antagónicos»), ou falhas do modelo.

CAPÍTULO 3
OBRIGAÇÕES DOS FORNECEDORES E UTILIZADORES DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO E DE OUTRAS PARTES

Artigo 16.º

Obrigações dos fornecedores de sistemas de inteligência artificial de risco elevado

Os fornecedores de sistemas de IA de risco elevado devem:

a)Assegurar que os seus sistemas de IA de risco elevado cumprem os requisitos estabelecidos no capítulo 2 do presente título;

b)Dispor de um sistema de gestão da qualidade que cumpra o disposto no artigo 17.º;

c)Elaborar a documentação técnica do sistema de IA de risco elevado;

d)Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem;

e)Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, antes da colocação no mercado ou da colocação em serviço;

f)Respeitar as obrigações de registo a que se refere o artigo 51.º;

g)Adotar as medidas corretivas necessárias, se o sistema de IA de risco elevado não estiver em conformidade com os requisitos estabelecidos no capítulo 2 do presente título;

h)Informar as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizaram o sistema de IA ou o colocaram em serviço e, se for caso disso, o organismo notificado sobre a não conformidade e quaisquer medidas corretivas tomadas;
i)Apor a marcação CE nos sistemas de IA de risco elevado para indicar a conformidade com o presente regulamento de acordo com o artigo 49.º;
j)Mediante pedido de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título.

Artigo 17.º
Sistema de gestão da qualidade

1.Os fornecedores de sistemas de IA de risco elevado devem criar um sistema de gestão da qualidade que assegure a conformidade com o presente regulamento. Esse sistema deve estar documentado de uma forma sistemática e ordenada, sob a forma de políticas, procedimentos e instruções escritas, e deve incluir, no mínimo, os seguintes aspetos:

a)Uma estratégia para o cumprimento da regulamentação, incluindo a observância de procedimentos de avaliação da conformidade e de procedimentos de gestão de modificações do sistema de IA de risco elevado;
b)Técnicas, procedimentos e ações sistemáticas a utilizar para a conceção, controlo da conceção e verificação da conceção do sistema de IA de risco elevado;
c)Técnicas, procedimentos e ações sistemáticas a utilizar para o desenvolvimento, controlo da qualidade e garantia da qualidade do sistema de IA de risco elevado;
d)Procedimentos de exame, teste e validação a realizar antes, durante e após o desenvolvimento do sistema de IA de risco elevado e a frequência com a qual têm de ser realizados;
e)Especificações técnicas, incluindo normas, a aplicar e, se as normas harmonizadas em causa não forem aplicadas na íntegra, os meios a usar para assegurar que o sistema de IA de risco elevado cumpra os requisitos estabelecidos no capítulo 2 do presente título;
f)Sistemas e procedimentos de gestão de dados, incluindo recolha de dados, análise de dados, rotulagem de dados, armazenamento de dados, filtragem de dados, prospeção de dados, agregação de dados, conservação de dados e qualquer outra operação relativa aos dados que seja realizada antes e para efeitos da colocação no mercado ou colocação em serviço de sistemas de IA de risco elevado;
g)O sistema de gestão de riscos a que se refere o artigo 9.º;
h)O estabelecimento, aplicação e manutenção de um sistema de acompanhamento pós-comercialização, nos termos do artigo 61.º;
i)Procedimentos de comunicação de incidentes graves e de anomalias em conformidade com o artigo 62.º;
j)A gestão da comunicação com autoridades nacionais competentes, autoridades competentes, incluindo as setoriais, disponibilizando ou apoiando o acesso a dados, organismos notificados, outros operadores, clientes ou outras partes interessadas;

k)Sistemas e procedimentos de manutenção de registos de toda a documentação e informação importante;
l)Gestão de recursos, incluindo medidas relacionadas com a segurança do aprovisionamento;
m)Um quadro que defina as responsabilidades do pessoal com funções de gestão e do restante pessoal no atinente a todos os aspetos elencados no presente número.

2.A aplicação dos aspetos referidos no n.º 1 deve ser proporcionada à dimensão da organização do fornecedor.

3.Em relação aos fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, considera-se que a obrigação de criar um sistema de gestão da qualidade é satisfeita mediante o cumprimento das regras relativas a sistemas, processos e mecanismos de governação interna previstas no artigo 74.º da referida diretiva. Neste contexto, devem ser tidas em conta quaisquer normas harmonizadas referidas no artigo 40.º do presente regulamento.

Artigo 18.º
Obrigação de elaborar documentação técnica

1.Os fornecedores de sistemas de IA de risco elevado devem elaborar a documentação técnica a que se refere o artigo 11.º de acordo com o anexo IV.

2.Os fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter a documentação técnica como parte da documentação relativa a sistemas, processos e mecanismos de governação interna elaborada nos termos do artigo 74.º da referida diretiva.

Artigo 19.º
Avaliação da conformidade

1.Os fornecedores de sistemas de IA de risco elevado devem assegurar que os sistemas que fornecem são sujeitos a um procedimento de avaliação da conformidade de acordo com o artigo 43.º, antes de serem colocados no mercado ou colocados em serviço. Assim que a conformidade dos sistemas de IA com os requisitos estabelecidos no capítulo 2 do presente título tiver sido demonstrada na sequência de uma avaliação da conformidade, os fornecedores devem elaborar uma declaração de conformidade UE de acordo com o artigo 48.º e apor a marcação de conformidade CE de acordo com o artigo 49.º.

2.Em relação aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, a avaliação da conformidade deve ser realizada no âmbito do procedimento a que se referem os artigos 97.º a 101.º da mesma diretiva.

Artigo 20.º
Registos gerados automaticamente

1.Os fornecedores de sistemas de IA de risco elevado devem manter os registos gerados automaticamente pelos respetivos sistemas de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal. Os registos devem ser mantidos por um período adequado em função da finalidade prevista do sistema de IA de risco elevado e das obrigações legais aplicáveis nos termos da legislação da União ou nacional.

2.Os fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter os registos gerados automaticamente pelos respetivos sistemas de IA de risco elevado como parte da documentação prevista no artigo 74.º da referida diretiva.

Artigo 21.º
Medidas corretivas

Os fornecedores de sistemas de IA de risco elevado que considerem ou tenham motivos para crer que um sistema de IA de risco elevado que colocaram no mercado ou colocaram em serviço não está em conformidade com o presente regulamento devem tomar imediatamente as medidas corretivas necessárias para repor a conformidade do sistema em questão ou proceder à retirada ou recolha do mesmo, consoante o caso. Devem igualmente informar do facto os distribuidores do sistema de IA de risco elevado em questão e, se for caso disso, o mandatário e os importadores.

Artigo 22.º
Dever de informação

Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, e esse risco for do conhecimento do fornecedor do sistema, este último deve informar imediatamente as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizou o sistema e, se for caso disso, o organismo notificado que emitiu um certificado para o sistema de IA de risco elevado, em especial sobre a não conformidade e quaisquer as medidas corretivas tomadas.

Artigo 23.º
Cooperação com as autoridades competentes

Os fornecedores de sistemas de IA de risco elevado devem, mediante pedido de uma autoridade nacional competente, prestar a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua oficial da União determinada pelo Estado-Membro em questão. Mediante pedido fundamentado de uma autoridade nacional competente, os fornecedores devem igualmente conceder a essa autoridade o acesso aos registos gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal.

Artigo 24.º
Obrigações dos fabricantes de produtos

Se um sistema de IA de risco elevado relacionado com produtos aos quais são aplicáveis os atos jurídicos enumerados no anexo II, secção A, for colocado no mercado ou colocado em serviço juntamente com o produto fabricado em conformidade com esses atos jurídicos e sob o nome do fabricante do produto, este último fica incumbido de garantir a conformidade do sistema de IA com o presente regulamento e, no que diz respeito ao sistema de IA, tem as mesmas obrigações impostas ao fornecedor pelo presente regulamento.

Artigo 25.º
Mandatários

1.Antes de disponibilizarem os seus sistemas no mercado da União, caso não seja possível identificar um importador, os fornecedores estabelecidos fora da

União devem, através de mandato escrito, designar um mandatário estabelecido na União.

2.O mandatário deve praticar os atos definidos no mandato conferido pelo fornecedor. O mandato deve habilitar o mandatário a exercer as seguintes funções:

a)Manter uma cópia da declaração de conformidade UE e da documentação técnica à disposição das autoridades nacionais competentes e das autoridades nacionais a que se refere o artigo 63.º, n.º 7;

b)Prestar a uma autoridade nacional competente, mediante pedido fundamentado, todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, incluindo o acesso aos registos gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos se encontrem sob o controlo do fornecedor por força de uma disposição contratual com o utilizador ou de uma disposição legal;

c)Cooperar com as autoridades nacionais competentes, mediante pedido fundamentado, em qualquer ação que estas empreendam em relação ao sistema de IA de risco elevado.

Artigo 26.º

Obrigações dos importadores

1.Antes de colocarem um sistema de IA de risco elevado no mercado, os importadores desse sistema devem assegurar-se de que:

a)O fornecedor desse sistema de IA realizou o procedimento de avaliação da conformidade adequado;

b)O fornecedor elaborou a documentação técnica em conformidade com o anexo IV;

c)O sistema ostenta a marcação de conformidade exigida e está acompanhado da documentação e das instruções de utilização necessárias.

2.Se um importador considerar ou tiver motivos para crer que um sistema de IA de risco elevado não está em conformidade com o presente regulamento, não pode colocar esse sistema de IA no mercado enquanto o mesmo não for tornado conforme. Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o importador deve informar desse facto o fornecedor do sistema de IA e as autoridades de fiscalização do mercado.

3.Os importadores devem indicar o seu nome, nome comercial registado ou marca registada e endereço de contacto no sistema de IA de risco elevado, ou, se tal não for possível, na respetiva embalagem ou na documentação que o acompanha, conforme aplicável.

4.Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos importadores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

5.Os importadores devem prestar às autoridades nacionais competentes, mediante pedido fundamentado, todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua que possa ser facilmente compreendida pela autoridade nacional competente em causa, incluindo o acesso aos registos gerados automaticamente

pelo sistema de IA de risco elevado, desde que esses registos se encontrem sob o controlo do fornecedor por força de uma disposição contratual com o utilizador ou de uma disposição legal. Devem igualmente cooperar com essas autoridades nacionais competentes em qualquer ação que estas empreendam em relação a esse sistema.

Artigo 27.º

Obrigações dos distribuidores

1.Antes de disponibilizarem um sistema de IA de risco elevado no mercado, os distribuidores devem verificar se o sistema de IA de risco elevado ostenta a marcação de conformidade CE exigida, se está acompanhado da documentação e das instruções de utilização necessárias e se o fornecedor e o importador do sistema, consoante o caso, cumpriram as obrigações estabelecidas no presente regulamento.

2.Se um distribuidor considerar ou tiver motivos para crer que um sistema de IA de risco elevado não está em conformidade com os requisitos estabelecidos no capítulo 2 do presente título, não pode disponibilizar esse sistema de IA de risco elevado no mercado enquanto o mesmo não for tornado conforme com os referidos requisitos. Além disso, se o sistema apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar desse facto o fornecedor ou o importador do sistema, conforme o caso.

3.Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos distribuidores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

4.Um distribuidor que considere ou tenha motivos para crer que um sistema de IA de risco elevado que disponibilizou no mercado não em conformidade com os requisitos estabelecidos no capítulo 2 do presente título deve tomar as medidas corretivas necessárias para repor a conformidade desse sistema com os referidos requisitos, proceder à retirada ou recolha do mesmo ou assegurar que o fornecedor, o importador ou qualquer operador envolvido, consoante o caso, toma essas medidas corretivas. Se um sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar imediatamente desse facto as autoridades nacionais competentes dos Estados-Membros em que disponibilizou o produto, apresentando dados, sobretudo no que se refere à não conformidade e às medidas corretivas tomadas.

5.Mediante pedido fundamentado de uma autoridade nacional competente, os distribuidores de sistemas de IA de risco elevado devem prestar a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título. Os distribuidores devem igualmente cooperar com essa autoridade nacional competente em qualquer ação que esta empreenda.

Artigo 28.º

Obrigações dos distribuidores, importadores, utilizadores e outros terceiros

1.Qualquer distribuidor, importador, utilizador ou outro terceiro será considerado um fornecedor para efeitos do presente regulamento e ficará sujeito às obrigações do fornecedor estabelecidas no artigo 16.º em qualquer uma das seguintes circunstâncias:

a)Se coloca no mercado ou colocar em serviço um sistema de IA de risco elevado sob o seu nome ou marca;

b)Se modificar a finalidade prevista de um sistema de IA de risco elevado já colocado no mercado ou colocado em serviço;

c)Se introduzir uma modificação substancial no sistema de IA de risco elevado.

2.Sempre que se verificarem as circunstâncias a que se refere o n.º 1, alíneas b) ou c), o fornecedor que inicialmente colocou no mercado ou colocou em serviço o sistema de IA de risco elevado deixará de ser considerado um fornecedor para efeitos do presente regulamento.

Artigo 29.º

Obrigações dos utilizadores de sistemas de inteligência artificial de risco elevado

1.Os utilizadores de sistemas de IA de risco elevado devem utilizá-los de acordo com as instruções de utilização que acompanham os sistemas, nos termos dos n.os 2 e 5.

2.As obrigações previstas no n.º 1 não excluem outras obrigações do utilizador previstas na legislação da União ou nacional nem prejudicam o poder discricionário do utilizador para organizar os seus próprios recursos e atividades para efeitos de aplicação das medidas de supervisão humana indicadas pelo fornecedor.

3.Sem prejuízo do disposto no n.º 1, desde que o utilizador exerça controlo sobre os dados de entrada, esse utilizador deve assegurar que os dados de entrada sejam adequados à finalidade prevista do sistema de IA de risco elevado.

4.Os utilizadores devem controlar o funcionamento do sistema de IA de risco elevado com base nas instruções de utilização. Se tiverem motivos para considerar que a utilização de acordo com as instruções de utilização pode fazer com que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, devem informar o fornecedor ou distribuidor e suspender a utilização do sistema. Devem também informar o fornecedor ou distribuidor e interromper a utilização do sistema de IA caso identifiquem qualquer incidente grave ou anomalia na aceção do artigo 62.º. Se o utilizador não conseguir entrar em contacto com o fornecedor, aplica-se, por analogia, o artigo 62.º.

Em relação aos utilizadores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, considera-se que a obrigação de controlo estabelecida no primeiro parágrafo é satisfeita mediante o cumprimento das regras relativas a sistemas, processos e mecanismos de governação interna previstas no artigo 74.º da referida diretiva.

5.Os utilizadores de sistemas de IA de risco elevado devem manter os registos gerados automaticamente por esse sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo. Os registos devem ser mantidos por um período adequado em função da finalidade prevista do sistema de IA de risco elevado e das obrigações legais aplicáveis nos termos da legislação da União ou nacional.

Os utilizadores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter os registos como parte da documentação relativa a sistemas, processos e mecanismos de governação interna prevista no artigo 74.º da referida diretiva.

6.Os utilizadores de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º para cumprirem a sua obrigação de realizar

uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, conforme aplicável.

CAPÍTULO 4
AUTORIDADES NOTIFICADORAS E ORGANISMOS NOTIFICADOS

Artigo 30.º
Autoridades notificadoras

1.Cada Estado-Membro deve designar ou criar uma autoridade notificadora responsável por estabelecer e executar os procedimentos necessários para a avaliação, a designação e a notificação de organismos de avaliação da conformidade e pela fiscalização destes.
2.Os Estados-Membros podem designar um organismo nacional de acreditação a que se refere o Regulamento (CE) n.º 765/2008 como autoridade notificadora.
3.As autoridades notificadoras devem ser criadas, organizadas e geridas de maneira que garanta a ausência de conflitos de interesses com os organismos de avaliação da conformidade e a objetividade e imparcialidade das suas atividades.
4.As autoridades notificadoras devem estar organizadas de maneira que as decisões relativas à notificação dos organismos de avaliação da conformidade sejam tomadas por pessoas competentes diferentes daquelas que realizaram a avaliação desses organismos.
5.As autoridades notificadoras não podem propor nem desempenhar qualquer atividade que seja da competência dos organismos de avaliação da conformidade, nem prestar quaisquer serviços de consultoria com caráter comercial ou em regime de concorrência.
6.As autoridades notificadoras devem proteger a confidencialidade das informações obtidas.
7.As autoridades notificadoras devem dispor de recursos humanos com competência técnica em número suficiente para o correto exercício das suas funções.
8.As autoridades notificadoras devem certificar-se de que as avaliações da conformidade são realizadas de modo proporcionado, evitando encargos desnecessários para os fornecedores, e de que os organismos notificados executam as suas atividades tendo devidamente em conta a dimensão da empresa, o setor no qual opera, a sua estrutura e o grau de complexidade do sistema de IA em apreço.

Artigo 31.º
Apresentação de pedido de notificação por um organismo de avaliação da conformidade

1.Os organismos de avaliação da conformidade devem apresentar um pedido de notificação à autoridade notificadora do Estado-Membro onde se encontram estabelecidos.
2.O pedido de notificação deve ser acompanhado de uma descrição das atividades de avaliação da conformidade, do módulo ou dos módulos de avaliação da conformidade e das tecnologias de inteligência artificial em relação às quais o organismo se considera competente, bem como de um certificado de acreditação, se existir, emitido por um organismo nacional de acreditação, que ateste que o organismo de avaliação da conformidade cumpre os requisitos estabelecidos no artigo 33.º Deve ser igualmente anexado qualquer documento

válido relacionado com designações vigentes do organismo notificado requerente ao abrigo de qualquer outra legislação de harmonização da União.
3.Se não lhe for possível apresentar o certificado de acreditação, o organismo de avaliação da conformidade deve fornecer à autoridade notificadora as provas documentais necessárias à verificação, ao reconhecimento e à fiscalização regular da sua conformidade com os requisitos estabelecidos no artigo 33.º. Em relação aos organismos notificados designados ao abrigo de qualquer outra legislação de harmonização da União, todos os documentos e certificados associados a essas designações podem ser usados para fundamentar o seu processo de designação nos termos do presente regulamento, consoante adequado.

Artigo 32.º
Procedimento de notificação

1.As autoridades notificadoras só podem notificar organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 33.º.
2.As autoridades notificadoras devem notificar a Comissão e os restantes Estados-Membros utilizando um instrumento de notificação eletrónica criado e gerido pela Comissão.
3.A notificação deve incluir dados completos das atividades de avaliação da conformidade, do módulo ou módulos de avaliação da conformidade e das tecnologias de inteligência artificial em questão.
4.O organismo de avaliação da conformidade em causa apenas pode exercer as atividades de organismo notificado se nem a Comissão nem os restantes Estados-Membros tiverem levantado objeções no mês seguinte à notificação.
5.As autoridades notificadoras devem comunicar à Comissão e aos restantes Estados-Membros todas as alterações importantes subsequentemente introduzidas na notificação.

Artigo 33.º
Organismos notificados

1.Os organismos notificados devem verificar a conformidade de um sistema de IA de risco elevado de acordo com os procedimentos de avaliação da conformidade a que se refere o artigo 43.º.
2.Os organismos notificados devem satisfazer os requisitos em termos de organização, gestão da qualidade, recursos e processos que sejam necessários para o exercício das suas tarefas.
3.A estrutura organizacional, a atribuição de responsabilidades, a cadeia hierárquica e o funcionamento dos organismos notificados devem ser de molde a assegurar a confiança no desempenho e nos resultados das atividades de avaliação da conformidade que os organismos notificados realizam.
4.Os organismos notificados devem ser independentes do fornecedor de um sistema de IA de risco elevado relativamente ao qual realizam atividades de avaliação da conformidade. Os organismos notificados devem também ser independentes de qualquer outro operador que tenha um interesse económico no sistema de IA de risco elevado que é avaliado, bem como de quaisquer concorrentes do fornecedor.
5.Os organismos notificados devem estar organizados e funcionar de maneira que garanta a independência, a objetividade e a imparcialidade das suas atividades. Os organismos notificados devem documentar e estabelecer uma estrutura e procedimentos capazes de salvaguardar essa imparcialidade e de

promover e aplicar os princípios da imparcialidade em toda a sua organização, pessoal e atividades de avaliação.
6.Os organismos notificados devem dispor de procedimentos documentados que garantam que o seu pessoal, comités, filiais, subcontratantes e qualquer outro organismo associado ou pessoal de organismos externos respeitam a confidencialidade das informações de que tenham conhecimento durante a realização das atividades de avaliação da conformidade, salvo se a divulgação daquelas for exigida por lei. O pessoal dos organismos notificados deve estar sujeito ao sigilo profissional no que se refere a todas as informações que obtiver no exercício das suas funções no âmbito do presente regulamento, exceto em relação às autoridades notificadoras do Estado-Membro em que exerce as suas atividades.
7.Os organismos notificados devem dispor de procedimentos relativos ao exercício de atividades que tenham em devida conta a dimensão de uma empresa, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA em questão.
8.Os organismos notificados devem subscrever um seguro de responsabilidade civil adequado para as suas atividades de avaliação da conformidade, a menos que essa responsabilidade seja assumida pelo Estado-Membro em causa nos termos da legislação nacional ou que esse Estado-Membro seja diretamente responsável pela avaliação da conformidade.
9.Os organismos notificados devem ser capazes de executar todas as tarefas que lhes forem atribuídas pelo presente regulamento com a maior integridade profissional e a competência exigida no domínio específico, quer essas tarefas sejam executadas por eles próprios, quer em seu nome e sob a sua responsabilidade.
10.Os organismos notificados devem dispor de competências internas suficientes para poderem avaliar eficazmente as tarefas realizadas em seu nome por partes externas. Para o efeito, em todas as circunstâncias e para cada procedimento de avaliação da conformidade e cada tipo de sistema de IA de risco elevado para os quais tenham sido designados, os organismos notificados devem dispor permanentemente de suficiente pessoal administrativo, técnico e científico com experiência e conhecimentos relativos às tecnologias de inteligência artificial em apreço, aos dados e à computação de dados e aos requisitos estabelecidos no capítulo 2 do presente título.
11.Os organismos notificados devem participar em atividades de coordenação conforme referido no artigo 38.º. Além disso, devem participar, diretamente ou por meio de representantes, em organizações europeias de normalização, ou assegurar que têm conhecimentos e se mantêm atualizados acerca das normas aplicáveis.
12.Os organismos notificados devem disponibilizar e, mediante pedido, apresentar toda a documentação importante, incluindo a documentação elaborada pelos fornecedores, à autoridade notificadora a que se refere o artigo 30.º para que esta possa exercer as suas atividades de avaliação, designação, notificação, controlo e fiscalização e ainda para facilitar a avaliação descrita no presente capítulo.

Artigo 34.º

Filiais e subcontratantes dos organismos notificados

1.Sempre que um organismo notificado subcontratar tarefas específicas relacionadas com a avaliação da conformidade ou recorrer a uma filial, deve

assegurar que o subcontratante ou a filial cumprem os requisitos previstos no artigo 33.º e informar a autoridade notificadora desse facto.
2.Os organismos notificados devem assumir plena responsabilidade pelas tarefas executadas por subcontratantes ou filiais, independentemente do local em que estes se encontram estabelecidos.
3.As atividades só podem ser exercidas por um subcontratante ou por uma filial mediante acordo do fornecedor.
4.Os organismos notificados devem manter à disposição da autoridade notificadora os documentos necessários respeitantes à avaliação das qualificações do subcontratante ou da filial e ao trabalho efetuado por estes nos termos do presente regulamento.

Artigo 35.º

Números de identificação e listas de organismos notificados designados nos termos do presente regulamento

1.A Comissão atribui um número de identificação aos organismos notificados. O número atribuído é único, mesmo que o organismo esteja notificado ao abrigo de vários atos da União.
2.A Comissão publica a lista de organismos notificados ao abrigo do presente regulamento, incluindo os números de identificação que lhes foram atribuídos e as atividades em relação às quais foram notificados. A Comissão assegura a atualização dessa lista.

Artigo 36.º

Alterações das notificações

1.Caso uma autoridade notificadora suspeite ou seja informada de que um organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 33.º, ou de que não cumpre as suas obrigações, deve imediatamente investigar a matéria com a máxima diligência. Neste contexto, deve informar o organismo notificado em causa sobre as objeções levantadas e dar-lhe a possibilidade de expressar as suas observações. Caso a autoridade notificadora conclua que o organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 33.º, ou que não cumpre as suas obrigações, deve restringir, suspender ou retirar a notificação, consoante o caso, em função da gravidade do incumprimento. Deve ainda informar imediatamente a Comissão e os restantes Estados-Membros deste facto.
2.Em caso de restrição, suspensão ou retirada da notificação, ou caso o organismo notificado tenha cessado atividade, a autoridade notificadora deve tomar as medidas necessárias para assegurar que os processos desse organismo notificado são assumidos por outro organismo notificado ou mantidos à disposição das autoridades notificadoras competentes, se estas o solicitarem.

Artigo 37.º

Contestação da competência dos organismos notificados

1.A Comissão investiga, sempre que necessário, todos os casos em que haja motivos para duvidar do cumprimento dos requisitos estabelecidos no artigo 33.º por parte de um organismo notificado.
2.A autoridade notificadora deve facultar à Comissão, mediante pedido, todas as informações importantes relacionadas com a notificação do organismo notificado em causa.

3.A Comissão garante que todas as informações confidenciais obtidas no decurso das suas investigações nos termos do presente artigo são tratadas de forma confidencial.

4.Caso verifique que um organismo notificado não cumpre ou deixou de cumprir os requisitos estabelecidos no artigo 33.º, a Comissão adota uma decisão fundamentada solicitando ao Estado-Membro notificador que tome as medidas corretivas necessárias, incluindo, se for caso disso, a retirada da notificação. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 38.º

Coordenação dos organismos notificados

1.A Comissão assegura que, no respeitante aos domínios abrangidos pelo presente regulamento, são instituídas modalidades de coordenação e cooperação adequadas entre organismos notificados ativos nos procedimentos de avaliação da conformidade de sistemas de IA nos termos do presente regulamento e que as mesmas decorrem devidamente sob a forma de um grupo setorial de organismos notificados.

2.Os Estados-Membros devem assegurar que os organismos por si notificados participam, diretamente ou por meio de representantes designados, nos trabalhos desse grupo.

Artigo 39.º

Organismos de avaliação da conformidade de países terceiros

Os organismos de avaliação da conformidade criados ao abrigo da legislação de um país terceiro com o qual a União tenha celebrado um acordo podem ser autorizados a executar as atividades de organismos notificados nos termos do presente regulamento.

CAPÍTULO 5
NORMAS, AVALIAÇÃO DA CONFORMIDADE, CERTIFICADOS, REGISTO

Artigo 40.º

Normas harmonizadas

Presume-se que os sistemas de IA de risco elevado que estão em conformidade com normas harmonizadas, ou com partes destas, cujas referências tenham sido publicadas no Jornal Oficial da União Europeia, são conformes com os requisitos estabelecidos no capítulo 2 do presente título, desde que tais normas abranjam esses requisitos.

Artigo 41.º

Especificações comuns

1.Na ausência das normas harmonizadas a que se refere o artigo 40.º ou caso a Comissão considere que as normas harmonizadas existentes são insuficientes ou que é necessário abordar preocupações específicas em termos de segurança ou direitos fundamentais, a Comissão pode, por meio de atos de execução, adotar especificações comuns relativas aos requisitos estabelecidos no capítulo 2 do presente título. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

2.Ao preparar as especificações comuns a que se refere o n.º 1, a Comissão recolhe as opiniões dos organismos ou grupos de peritos pertinentes criados nos termos do direito setorial da União aplicável.

3.Presume-se que os sistemas de IA de risco elevado que estão em conformidade com as especificações comuns a que se refere o n.º 1 são conformes com os

requisitos estabelecidos no capítulo 2 do presente título, desde que tais especificações comuns abranjam esses requisitos.

4.Os fornecedores que não cumprirem as especificações comuns a que se refere o n.º 1 devem justificar devidamente que adotaram soluções técnicas, no mínimo, equivalentes.

Artigo 42.º

Presunção de conformidade com determinados requisitos

1.Tendo em conta a sua finalidade prevista, presume-se que os sistemas de IA de risco elevado que foram treinados e testados com recurso a dados relativos ao enquadramento geográfico, comportamental e funcional específico no qual se destinam a ser utilizados são conformes com o requisito estabelecido no artigo 10.º, n.º 4.

2.Presume-se que os sistemas de IA de risco elevado que foram certificados ou relativamente aos quais foi emitida uma declaração de conformidade no âmbito de um sistema de certificação da cibersegurança estabelecido nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho 63 e cujas referências foram publicadas no Jornal Oficial da União Europeia são conformes com os requisitos de cibersegurança estabelecidos no artigo 15.º do presente regulamento, contanto que o certificado de cibersegurança ou a declaração de conformidade ou partes dos mesmos abranjam esses requisitos.

Artigo 43.º

Avaliação da conformidade

1.No respeitante aos sistemas de IA de risco elevado enumerados no anexo III, ponto 1, quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor tiver aplicado normas harmonizadas a que se refere o artigo 40.º, ou, se for caso disso, especificações comuns a que se refere o artigo 41.º, o fornecedor deve seguir um dos seguintes procedimentos:

a)O procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI;

b)O procedimento de avaliação da conformidade baseado na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica, com a participação de um organismo notificado, a que se refere o anexo VII.

Quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor não tiver aplicado ou tiver aplicado apenas parcialmente normas harmonizadas a que se refere o artigo 40.º, ou se tais normas harmonizadas não existirem e as especificações comuns a que se refere o artigo 41.º não estiverem disponíveis, o fornecedor deve seguir o procedimento de avaliação da conformidade preconizado no anexo VII.

Para efeitos do procedimento de avaliação da conformidade a que se refere o anexo VII, o fornecedor pode escolher qualquer um dos organismos notificados. Contudo, se o sistema se destinar a ser colocado em serviço por autoridades competentes em matéria de manutenção da ordem pública, imigração ou asilo, bem como por instituições, órgãos e organismos da UE, a autoridade de fiscalização do mercado a que se refere o artigo 63.º, n.os 5 ou 6, consoante o caso, deve atuar como um organismo notificado.

2.Em relação aos sistemas de IA de risco elevado enumerados no anexo III, pontos 2 a 8, os fornecedores devem seguir o procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI, que não prevê a participação de um organismo notificado. Em relação aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), que são colocados no mercado ou colocados em serviço por instituições de crédito regulamentadas pela Diretiva 2013/36/UE, a avaliação da conformidade deve ser realizada no âmbito do procedimento a que se referem os artigos 97.º a 101.º da mesma diretiva.

3.Em relação aos sistemas de IA de risco elevado aos quais são aplicáveis atos jurídicos enumerados no anexo II, secção A, o fornecedor deve seguir o procedimento de avaliação da conformidade aplicável nos termos desses atos jurídicos. Os requisitos estabelecidos no capítulo 2 do presente título aplicam-se a esses sistemas de IA de risco elevado e devem fazer parte dessa avaliação. É igualmente aplicável o disposto no anexo VII, pontos 4.3, 4.4, 4.5, e ponto 4.6, quinto parágrafo.

Para efeitos dessa avaliação, os organismos notificados que tenham sido notificados ao abrigo dos referidos atos jurídicos ficam habilitados a verificar a conformidade dos sistemas de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, contanto que a conformidade desses organismos notificados com os requisitos estabelecidos no artigo 33.º, n.os 4, 9 e 10, tenha sido avaliada no contexto do procedimento de notificação previsto nesses atos jurídicos.

Sempre que os atos jurídicos enumerados no anexo II, secção A, permitam ao fabricante do produto renunciar a uma avaliação da conformidade por terceiros, desde que tenha aplicado todas as normas harmonizadas que abrangem os requisitos previstos nesses atos, esse fabricante apenas pode fazer uso de tal opção se tiver também aplicado normas harmonizadas ou, se for caso disso, especificações comuns a que se refere o artigo 41.º que abranjam os requisitos estabelecidos no capítulo 2 do presente título.

4.Os sistemas de IA de risco elevado devem ser sujeitos a um novo procedimento de avaliação da conformidade sempre que forem substancialmente modificados, independentemente de o sistema modificado se destinar a distribuição ulterior ou continuar a ser usado pelo utilizador atual.

No respeitante aos sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço, as alterações introduzidas no sistema de IA de risco elevado e no seu desempenho que tenham sido predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial e façam parte das informações contidas na documentação técnica a que se refere o anexo VI, ponto 2, alínea f), não constituem uma modificação substancial.

5.A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar os anexos VI e VII, a fim de introduzir elementos dos procedimentos de avaliação da conformidade que se tornem necessários à luz da evolução técnica.

6.A Comissão fica habilitada a adotar atos delegados para alterar os n.os 1 e 2, a fim de sujeitar os sistemas de IA de risco elevado referidos no anexo III, pontos 2 a 8, ao procedimento de avaliação da conformidade referido no anexo VII ou a partes daquele. A Comissão adota esses atos delegados tendo em conta a eficácia do procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI na prevenção ou minimização dos riscos para

a saúde e a segurança e a proteção dos direitos fundamentais representados por esses sistemas, bem como a disponibilidade de capacidades e recursos adequados entre os organismos notificados.

Artigo 44.º
Certificados

1.Os certificados emitidos por organismos notificados nos termos do anexo VII devem ser redigidos numa língua oficial da União determinada pelo Estado-Membro em que estiver estabelecido o organismo notificado ou numa outra língua oficial da União aceite pelo organismo notificado.
2.Os certificados são válidos pelo período neles indicado, que não pode exceder cinco anos. A pedido do fornecedor, a validade de um certificado pode ser prorrogada por novos períodos não superiores a cinco anos, com base numa reavaliação segundo os procedimentos de avaliação da conformidade aplicáveis.
3.Se verificar que um sistema de IA deixou de cumprir os requisitos estabelecidos no capítulo 2 do presente título, o organismo notificado deve suspender, retirar ou restringir o certificado emitido, tendo em conta o princípio da proporcionalidade, a não ser que o fornecedor do sistema garanta o cumprimento desses requisitos tomando as medidas corretivas necessárias num prazo adequado estabelecido pelo organismo notificado. O organismo notificado deve fundamentar a sua decisão.

Artigo 45.º
Recurso das decisões dos organismos notificados

Os Estados-Membros devem assegurar a disponibilidade de um procedimento de recurso das decisões às partes com um interesse legítimo nessa decisão.

Artigo 46.º
Obrigações de informação dos organismos notificados

1.Os organismos notificados devem comunicar à autoridade notificadora as seguintes informações:

a)Certificados da União de avaliação da documentação técnica, todos os suplementos desses certificados, bem como aprovações do sistema de gestão da qualidade emitidos de acordo com os requisitos do anexo VII;

b)Recusas, restrições, suspensões ou retiradas de certificados da União de avaliação da documentação técnica ou de aprovações de sistemas de gestão da qualidade emitidos em conformidade com os requisitos constantes do anexo VII;

c)As circunstâncias que afetem o âmbito ou as condições de notificação;

d)Pedidos de informação que tenham recebido das autoridades de fiscalização do mercado sobre as atividades de avaliação da conformidade;

e)Se lhes for solicitado, as atividades de avaliação da conformidade realizadas no âmbito da respetiva notificação e quaisquer outras atividades exercidas, nomeadamente atividades transfronteiras e de subcontratação.

2.Cada organismo notificado deve informar os outros organismos notificados sobre:

a)As aprovações de sistemas de gestão da qualidade que tenha recusado, suspendido ou retirado e, se lhe for pedido, as aprovações que tenha concedido a sistemas de qualidade;

b)Os certificados UE de avaliação da documentação técnica ou quaisquer suplementos dos mesmos que tenha recusado, retirado, suspendido ou

restringido de outro modo e, se lhe for pedido, os certificados e/ou suplementos dos mesmos que tenha emitido.

3.Cada organismo notificado deve disponibilizar aos outros organismos notificados que realizam atividades de avaliação da conformidade semelhantes, abrangendo as mesmas tecnologias de inteligência artificial, informações importantes sobre questões relativas aos resultados negativos e, se lhe for pedido, aos resultados positivos de procedimentos de avaliação da conformidade.

Artigo 47.º

Derrogação do procedimento de avaliação da conformidade

1.Em derrogação do artigo 43.º, qualquer autoridade de fiscalização do mercado pode autorizar a colocação no mercado ou a colocação em serviço de determinados sistemas de IA de risco elevado no território do Estado-Membro em causa, por motivos excecionais de segurança pública ou de proteção da vida e da saúde das pessoas, de proteção do ambiente e de proteção de ativos industriais e infraestruturas essenciais. Essa autorização deve ser concedida por um período limitado, enquanto os procedimentos de avaliação da conformidade necessários estiverem a ser executados, e cessa assim que esses procedimentos tiverem sido concluídos. A conclusão desses procedimentos deve ser realizada sem demora injustificada.

2.A autorização a que se refere o n.º 1 apenas deve ser concedida se a autoridade de fiscalização do mercado concluir que o sistema de IA de risco elevado cumpre os requisitos do capítulo 2 do presente título. A autoridade de fiscalização do mercado deve informar a Comissão e os outros Estados-Membros sobre qualquer autorização concedida nos termos do n.º 1.

3.Se, no prazo de 15 dias a contar da receção da informação a que se refere o n.º 2, nem os Estados-Membros nem a Comissão tiverem levantado objeções a uma autorização concedida por uma autoridade de fiscalização do mercado de um Estado-Membro em conformidade com o n.º 1, considera-se que a mesma é justificada.

4.Se, nos 15 dias subsequentes à receção da notificação a que se refere o n.º 2, um Estado-Membro levantar objeções a uma autorização concedida por uma autoridade de fiscalização do mercado de outro Estado-Membro, ou se a Comissão considerar que a autorização é contrária ao direito da União ou que a conclusão dos Estados-Membros relativa à conformidade do sistema a que se refere o n.º 2 é infundada, a Comissão procede sem demora a consultas com o Estado-Membro em causa. Os operadores em questão devem ser consultados e ter a possibilidade de apresentar as suas observações. Tendo em conta essas observações, a Comissão decide se a autorização se justifica ou não. A Comissão designa o Estado-Membro e o operador ou operadores em causa como destinatários da decisão.

5.Se a autorização for considerada injustificada, a autoridade de fiscalização do mercado do Estado-Membro em causa deve retirá-la.

6.Em derrogação dos n.os 1 a 5, no respeitante a sistemas de IA de risco elevado concebidos para serem usados como componentes de segurança de dispositivos ou que sejam, eles próprios, dispositivos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, o artigo 59.º do Regulamento (UE) 2017/745 e o artigo 54.º do Regulamento (UE) 2017/746 também são aplicáveis no atinente à derrogação da avaliação da conformidade do cumprimento dos requisitos estabelecidos no capítulo 2 do presente título.

Artigo 48.º

Declaração de conformidade UE

1.O fornecedor deve elaborar uma declaração de conformidade UE escrita para cada sistema de IA e mantê-la à disposição das autoridades nacionais competentes por um período de dez anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA. A declaração de conformidade UE deve especificar o sistema de IA para o qual foi elaborada. Deve ser fornecida uma cópia da declaração de conformidade UE às autoridades nacionais competentes, mediante pedido.

2.A declaração de conformidade UE deve mencionar que o sistema de IA de risco elevado em questão cumpre os requisitos estabelecidos no capítulo 2 do presente título. A declaração de conformidade UE deve conter as informações indicadas no anexo V e ser traduzida para uma ou várias línguas oficiais da União exigidas pelos Estados-Membros em que o sistema de IA de risco elevado é disponibilizado.

3.Se os sistemas de IA de risco elevado estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração de conformidade UE, deve ser elaborada uma única declaração de conformidade UE respeitante a todos os atos jurídicos da UE aplicáveis ao sistema de IA de risco elevado. A declaração deve incluir todas as informações necessárias para identificar a legislação de harmonização da União a que diz respeito.

4.Ao elaborar a declaração de conformidade UE, o fornecedor deve assumir a responsabilidade pelo cumprimento dos requisitos estabelecidos no capítulo 2 do presente título. O fornecedor deve manter a declaração de conformidade UE atualizada, consoante necessário.

5.A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar o conteúdo da declaração de conformidade UE preconizado no anexo V, a fim de introduzir elementos que se tornem necessários à luz da evolução técnica.

Artigo 49.º

Marcação de conformidade CE

1.A marcação CE deve ser aposta de modo visível, legível e indelével em sistemas de IA de risco elevado. Caso a natureza do sistema de IA de risco elevado não permita ou não garanta essas características da marcação, esta deve ser aposta na embalagem ou na documentação que acompanha o sistema, conforme mais adequado.

2.A marcação CE a que se refere o n.º 1 está sujeita aos princípios gerais estabelecidos no artigo 30.º do Regulamento (CE) n.º 765/2008.

3.Quando aplicável, a marcação CE deve ser seguida pelo número de identificação do organismo notificado responsável pelos procedimentos de avaliação da conformidade estabelecidos no artigo 43.º. O número de identificação deve ser igualmente indicado em qualquer material promocional que mencione que o sistema de IA de risco elevado cumpre os requisitos aplicáveis à marcação CE.

Artigo 50.º

Conservação de documentos

O fornecedor deve manter à disposição das autoridades nacionais competentes, durante os dez anos subsequentes à data de colocação no mercado ou de colocação em serviço do sistema de IA:

a)A documentação técnica a que se refere o artigo 11.º;

b)A documentação relativa ao sistema de gestão da qualidade a que se refere o artigo 17.º;
c)A documentação relativa às alterações aprovadas pelos organismos notificados, se for caso disso;
d)As decisões e outros documentos emitidos pelos organismos notificados, se for caso disso;
e)A declaração de conformidade UE a que se refere o artigo 48.º.

Artigo 51.º
Registo

Antes da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado referido no artigo 6.º, n.º 2, o fornecedor ou, se for caso disso, o mandatário deve registar esse sistema na base de dados da UE a que se refere o artigo 60.º.

TÍTULO IV
OBRIGAÇÕES DE TRANSPARÊNCIA APLICÁVEIS A DETERMINADOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Artigo 52.º
Obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial

1.Os fornecedores devem assegurar que os sistemas de IA destinados a interagir com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares sejam informadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio dadas as circunstâncias e o contexto de utilização. Esta obrigação não se aplica a sistemas de IA legalmente autorizados para detetar, prevenir, investigar e reprimir infrações penais, salvo se esses sistemas estiverem disponíveis ao público para denunciar uma infração penal.
2.Os utilizadores de um sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas. Esta obrigação não se aplica a sistemas de IA usados para categorização biométrica que sejam legalmente autorizados para detetar, prevenir e investigar infrações penais.
3.Os utilizadores de um sistema de IA que gera ou manipula conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, objetos, locais ou outras entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa («falsificação profunda») devem divulgar que o conteúdo foi gerado ou manipulado artificialmente.
Contudo, o primeiro parágrafo não se aplica se a utilização for legalmente autorizada para detetar, prevenir, investigar e reprimir infrações penais ou for necessária para exercer o direito à liberdade de expressão e o direito à liberdade das artes e das ciências consagrados na Carta dos Direitos Fundamentais da UE, desde que salvaguarde adequadamente os direitos e as liberdades de terceiros.
4.Os n.os 1, 2 e 3 não afetam os requisitos e as obrigações estabelecidos no título III do presente regulamento.

TÍTULO V
MEDIDAS DE APOIO À INOVAÇÃO

Artigo 53.º

Ambientes de testagem da regulamentação da inteligência artificial

1.Os ambientes de testagem da regulamentação da IA estabelecidos pelas autoridades competentes de um ou vários Estados-Membros ou pela Autoridade Europeia para a Proteção de Dados devem proporcionar um ambiente controlado que facilite o desenvolvimento, a testagem e a validação de sistemas de IA inovadores por um período limitado antes da sua colocação no mercado ou colocação em serviço de acordo com um plano específico. Tal deve ocorrer sob a supervisão e orientação diretas das autoridades competentes com vista a garantir a conformidade com os requisitos do presente regulamento e, quando pertinente, de outra legislação da União e dos Estados-Membros supervisionada no ambiente de testagem.

2.Os Estados-Membros devem assegurar que, no caso de os sistemas de IA inovadores envolverem o tratamento de dados pessoais ou de outro modo se enquadrarem na competência de supervisão de outras autoridades nacionais ou autoridades competentes que disponibilizam ou apoiam o acesso a dados, as autoridades nacionais de proteção de dados e essas outras autoridades nacionais são associadas ao funcionamento do ambiente de testagem da regulamentação da IA.

3.Os ambientes de testagem da regulamentação da IA não afetam os poderes de supervisão e de correção das autoridades competentes. A identificação de quaisquer riscos significativos para a saúde e a segurança e os direitos fundamentais durante o desenvolvimento e a testagem desses sistemas deve conduzir à adoção imediata de medidas de atenuação e, na sua falta, à suspensão do processo de desenvolvimento e testagem até que se verifique essa atenuação.

4.Os participantes no ambiente de testagem da regulamentação da IA continuam a ser responsáveis, nos termos da legislação aplicável da União e dos Estados-Membros em matéria de responsabilidade, por quaisquer danos infligidos a terceiros em resultado da experimentação que ocorre no ambiente de testagem.

5.As autoridades competentes dos Estados-Membros que criaram ambientes de testagem da regulamentação da IA devem coordenar as suas atividades e cooperar no quadro do Comité Europeu para a Inteligência Artificial. Essas autoridades devem apresentar relatórios anuais ao Comité e à Comissão sobre os resultados da aplicação desse sistema, incluindo boas práticas, ensinamentos retirados e recomendações sobre a sua configuração e, se for caso disso, sobre a aplicação do presente regulamento e de outra legislação da União supervisionada no ambiente de testagem.

6.As modalidades e condições de funcionamento dos ambientes de testagem da regulamentação da IA, incluindo os critérios de elegibilidade e o procedimento de candidatura, seleção, participação e saída do ambiente de testagem, bem como os direitos e as obrigações dos participantes, devem ser estabelecidas em atos de execução. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 54.º

Tratamento adicional de dados pessoais para efeitos de desenvolvimento de certos sistemas de inteligência artificial de interesse público no ambiente de testagem da regulamentação da inteligência artificial

1.No ambiente de testagem da regulamentação da IA, os dados pessoais legalmente recolhidos para outras finalidades podem ser tratados com vista a desenvolver e testar certos sistemas de IA inovadores no ambiente de testagem nas seguintes condições:

a)Os sistemas de IA inovadores devem ser desenvolvidos para salvaguarda de um interesse público substancial num ou mais dos seguintes domínios:

i)prevenção, investigação, deteção ou repressão de infrações penais, ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas, sob o controlo e a responsabilidade das autoridades competentes. O tratamento obedece ao disposto na legislação do Estado-Membro ou da União,

ii)segurança pública e saúde pública, nomeadamente a prevenção, o controlo e o tratamento de doenças,

iii)elevado nível de proteção e melhoria da qualidade do ambiente;

b)Os dados tratados são necessários para cumprir um ou vários dos requisitos referidos no título III, capítulo 2, caso esses requisitos não possam ser eficazmente cumpridos mediante tratamento de dados anonimizados, sintéticos ou outros dados não pessoais;

c)Existem mecanismos de controlo eficazes para identificar quaisquer riscos elevados para os direitos fundamentais dos titulares dos dados que possam surgir durante a experimentação no ambiente de testagem, bem como um mecanismo de resposta para atenuar prontamente esses riscos e, se necessário, interromper o tratamento;

d)Todos os dados pessoais a tratar no contexto do ambiente de testagem se encontram num ambiente de tratamento de dados funcionalmente separado, isolado e protegido sob o controlo dos participantes, sendo apenas acessíveis a pessoas autorizadas;

e)Nenhuns dados pessoais tratados são transmitidos, transferidos ou acedidos, de outro modo, por terceiros;

f)Nenhum tratamento de dados pessoais no contexto do ambiente de testagem dá origem a medidas ou decisões que afetem os titulares dos dados;

g)Todos os dados pessoais tratados no contexto do ambiente de testagem são apagados assim que a participação no ambiente de testagem terminar ou que os dados pessoais atingirem o fim do respetivo período de conservação;

h)Os registos do tratamento de dados pessoais no contexto do ambiente de testagem são mantidos durante a participação no ambiente de testagem e pelo período de um ano após o respetivo termo, apenas enquanto forem necessários para efeitos exclusivos de cumprimento de obrigações em matéria de responsabilidade e documentação previstas no presente artigo ou em outra legislação da União ou dos Estados-Membros aplicável;

i)É mantida, juntamente com os resultados dos testes, uma descrição completa e pormenorizada do processo e da lógica subjacentes ao treino, ao teste e à validação do sistema de IA como parte da documentação técnica prevista no anexo IV;

j)Uma breve síntese do projeto de IA desenvolvido no ambiente de testagem, incluindo os seus objetivos e resultados esperados, é publicada no sítio Web das autoridades competentes.

2.O n.º 1 não prejudica a legislação da União ou dos Estados-Membros que exclui o tratamento para outras finalidades que não as explicitamente mencionadas nessa legislação.

Artigo 55.º

Medidas para fornecedores e utilizadores de pequena dimensão

1.Os Estados-Membros devem empreender as seguintes ações:

a)Proporcionar aos fornecedores de pequena dimensão e às empresas em fase de arranque acesso prioritário aos ambientes de testagem da regulamentação da IA, desde que cumpram as condições de elegibilidade;

b)Organizar atividades de sensibilização específicas sobre a aplicação do presente regulamento adaptadas às necessidades dos fornecedores e utilizadores de pequena dimensão;

c)Se for caso disso, criar um canal específico para comunicação com fornecedores e utilizadores de pequena dimensão e outros inovadores, com o intuito de fornecer orientações e responder a consultas sobre a aplicação do presente regulamento.

2.Os interesses e as necessidades específicas dos fornecedores de pequena dimensão devem ser tidas em conta aquando da fixação das taxas a pagar pela avaliação da conformidade nos termos do artigo 43.º, reduzindo essas taxas proporcionalmente à sua dimensão e à dimensão do mercado.

TÍTULO VI
GOVERNAÇÃO
CAPÍTULO 1
COMITÉ EUROPEU PARA A INTELIGÊNCIA ARTIFICIAL

Artigo 56.º

Criação do Comité Europeu para a Inteligência Artificial

1.É criado um Comité Europeu para a Inteligência Artificial (adiante designado por «Comité»).

2.O Comité presta aconselhamento e assistência à Comissão com vista a:

a)Contribuir para a cooperação eficaz entre as autoridades nacionais de controlo e a Comissão no tocante às matérias abrangidas pelo presente regulamento;

b)Coordenar e contribuir para a elaboração de orientações e análises por parte da Comissão e das autoridades nacionais de controlo, bem como de outras autoridades competentes, sobre questões emergentes no mercado interno no tocante às matérias abrangidas pelo presente regulamento;

c)Auxiliar as autoridades nacionais de controlo e a Comissão a garantirem a aplicação coerente do presente regulamento.

Artigo 57.º

Estrutura do Comité

1.O Comité é composto pelas autoridades nacionais de controlo, que são representadas pelo seu presidente ou funcionário de alto nível equivalente, e pela Autoridade Europeia para a Proteção de Dados. Podem ser convidadas para as reuniões outras autoridades nacionais, sempre que as questões debatidas sejam pertinentes para as mesmas.

2.O Comité adota o seu regulamento interno por maioria simples dos membros que o compõem, após a autorização da Comissão. O regulamento interno deve conter igualmente os aspetos operacionais relacionados com o exercício das

funções do Comité elencadas no artigo 58.º. O Comité pode constituir subgrupos consoante adequado para efeitos da análise de questões específicas.

3.O Comité é presidido pela Comissão. A Comissão convoca as reuniões e prepara a ordem de trabalhos de acordo com as funções do Comité nos termos do presente regulamento e com o seu regulamento interno. A Comissão presta apoio administrativo e analítico às atividades do Comité nos termos com o presente regulamento.

4.O Comité pode convidar peritos e observadores externos para participarem nas suas reuniões e pode realizar intercâmbios com terceiros interessados, a fim de fundamentar as suas atividades, na medida adequada. Para o efeito, a Comissão pode facilitar intercâmbios entre o Comité e outras instituições, órgãos, organismos e grupos consultivos da União.

Artigo 58.º

Funções do Comité

Ao prestar aconselhamento e assistência à Comissão nos termos do artigo 56.º, n.º 2, o Comité deve em particular:

a)Recolher e partilhar conhecimentos técnicos e boas práticas entre Estados-Membros;

b)Contribuir para uniformizar práticas administrativas nos Estados-Membros, nomeadamente no respeitante ao funcionamento dos ambientes de testagem da regulamentação a que se refere o artigo 53.º;

c)Emitir pareceres, recomendações ou contribuições escritas sobre matérias relacionadas com a aplicação do presente regulamento, em especial:

i)sobre especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no título III, capítulo 2,

ii)sobre a utilização de normas harmonizadas ou especificações comuns a que se referem os artigos 40.º e 41.º,

iii)sobre a preparação de documentos de orientação, nomeadamente as orientações relativas à fixação de coimas a que se refere o artigo 71.º.

CAPÍTULO 2

AUTORIDADES NACIONAIS COMPETENTES

Artigo 59.º

Designação das autoridades nacionais competentes

1.Cada Estado-Membro deve criar ou designar autoridades nacionais competentes a fim de assegurar a aplicação e execução do presente regulamento. As autoridades nacionais competentes devem estar organizadas de modo que garanta a objetividade e a imparcialidade das suas atividades e funções.

2.Cada Estado-Membro deve designar uma autoridade nacional de controlo entre as autoridades nacionais competentes. A autoridade nacional de controlo deve atuar enquanto autoridade notificadora e autoridade de fiscalização do mercado, salvo se, por razões organizacionais e administrativas, o Estado-Membro tiver de designar mais do que uma autoridade.

3.Os Estados-Membros devem informar a Comissão da designação ou designações e, se for caso disso, dos motivos que os levaram a designar mais do que uma autoridade.

4.Os Estados-Membros devem assegurar que as autoridades nacionais competentes disponham dos recursos financeiros e humanos adequados para exercerem as funções que lhes incumbem nos termos do presente regulamento.

Em especial, as autoridades nacionais competentes devem dispor permanentemente de suficiente pessoal cujas competências e conhecimentos especializados incluam uma compreensão profunda das tecnologias de inteligência artificial, dos dados e da computação de dados, dos direitos fundamentais e dos riscos para a saúde e a segurança, bem como conhecimento das normas e dos requisitos legais em vigor.

5.Os Estados-Membros devem apresentar anualmente relatórios à Comissão sobre a situação dos recursos financeiros e humanos ao dispor das autoridades nacionais competentes, incluindo uma avaliação da sua adequação. A Comissão transmite essas informações ao Comité para apreciação e eventuais recomendações.

6.A Comissão facilita o intercâmbio de experiências entre as autoridades nacionais competentes.

7.As autoridades nacionais competentes podem fornecer orientações e prestar aconselhamento sobre a execução do presente regulamento, nomeadamente aos fornecedores de pequena dimensão. Sempre que as autoridades nacionais competentes pretendam fornecer orientações e prestar aconselhamento em relação a um sistema de IA em domínios abrangidos por outra legislação da União, as autoridades nacionais competentes ao abrigo dessa legislação da União devem ser consultadas, conforme adequado. Os Estados-Membros também podem criar um ponto de contacto central para a comunicação com os operadores.

8.Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade competente para o controlo dos mesmos.

TÍTULO VII
BASE DE DADOS DA UE RELATIVA A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO AUTÓNOMOS

Artigo 60.º

Base de dados da UE relativa a sistemas de inteligência artificial de risco elevado autónomos

1.A Comissão, em colaboração com os Estados-Membros, cria e mantém uma base de dados da UE que contenha as informações referidas no n.º 2 relativas aos sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2, que sejam registados em conformidade com o artigo 51.º.

2.Cabe aos fornecedores introduzir os dados enumerados no anexo VIII na base de dados da UE. A Comissão faculta-lhes apoio técnico e administrativo.

3.As informações que constam da base de dados da UE devem estar acessíveis ao público.

4.A base de dados da UE só pode conter dados pessoais se estes forem necessários para recolher e tratar informações em conformidade com o presente regulamento. Essas informações incluem os nomes e os contactos das pessoas singulares responsáveis pelos registos no sistema e com autoridade jurídica para representar o fornecedor.

5.A Comissão é considerada responsável pelo tratamento de dados da base de dados da UE. Além disso, assegura aos fornecedores o apoio técnico e administrativo adequado.

TÍTULO VIII
ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO, PARTILHA DE INFORMAÇÕES, FISCALIZAÇÃO DO MERCADO

CAPÍTULO 1
ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO

Artigo 61.º

Acompanhamento pós-comercialização pelos fornecedores e plano de acompanhamento pós-comercialização aplicável a sistemas de inteligência artificial de risco elevado

1.Os fornecedores devem criar e documentar um sistema de acompanhamento pós-comercialização que seja proporcionado à natureza das tecnologias de inteligência artificial e aos riscos do sistema de IA de risco elevado.

2.O sistema de acompanhamento pós-comercialização deve recolher, documentar e analisar de forma ativa e sistemática dados pertinentes fornecidos pelos utilizadores ou recolhidos por meio de outras fontes sobre o desempenho dos sistemas de IA de risco elevado ao longo da sua vida útil, bem como permitir ao fornecedor avaliar a contínua conformidade dos sistemas de IA com os requisitos estabelecidos no título III, capítulo 2.

3.O sistema de monitorização pós-comercialização deve basear-se num plano de acompanhamento pós-comercialização. O plano de acompanhamento pós-comercialização deve fazer parte da documentação técnica referida no anexo IV. A Comissão adota um ato de execução com disposições pormenorizadas que estabeleçam um modelo para o plano de acompanhamento pós-comercialização e a lista de elementos a incluir no plano.

4.No respeitante aos sistemas de IA de risco elevado abrangidos pelos atos jurídicos referidos no anexo II, relativamente aos quais já se encontram estabelecidos um sistema e um plano de acompanhamento pós-comercialização ao abrigo dessa legislação, os elementos descritos nos n.os 1, 2 e 3 devem ser integrados nesse sistema e nesse plano, consoante adequado.

O primeiro parágrafo também é aplicável aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por instituições de crédito regulamentadas pela Diretiva 2013/36/UE.

CAPÍTULO 2
PARTILHA DE INFORMAÇÕES SOBRE INCIDENTES E ANOMALIAS

Artigo 62.º

Comunicação de incidentes graves e anomalias

1.Os fornecedores de sistemas de IA de risco elevado colocados no mercado da União devem comunicar quaisquer incidentes graves ou anomalias desses sistemas que constituam um incumprimento de obrigações impostas pela legislação da União destinada a proteger os direitos fundamentais às autoridades de fiscalização do mercado dos Estados-Membros onde esse incidente ou incumprimento ocorrer.

Essa notificação deve ser efetuada imediatamente após o fornecedor ter determinado uma relação causal entre o sistema de IA e o incidente ou anomalia ou a probabilidade razoável dessa relação e, em qualquer caso, o mais tardar 15 dias após o fornecedor ter conhecimento do incidente grave ou da anomalia.

2.Após receção de uma notificação relacionada com um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais, a autoridade de fiscalização do mercado deve informar as autoridades ou os organismos públicos nacionais referidos no artigo 64.º, n.º 3.

A Comissão elabora orientações específicas para facilitar o cumprimento das obrigações previstas no n.º 1. As referidas orientações devem ser publicadas, o mais tardar, 12 meses após a entrada em vigor do presente regulamento.

3.Relativamente aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE e relativamente aos sistemas de IA de risco elevado que sejam componentes de segurança de dispositivos ou sejam, eles próprios, dispositivos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, a notificação de incidentes graves ou anomalias limita-se aos casos que constituam um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais.

CAPÍTULO 3
EXECUÇÃO

Artigo 63.º

Fiscalização do mercado e controlo dos sistemas de inteligência artificial presentes no mercado da União

1.O Regulamento (UE) 2019/1020 é aplicável aos sistemas de IA abrangidos pelo presente regulamento. Contudo, para efeitos da execução efetiva do presente regulamento:

a)Qualquer referência a um operador económico nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os operadores identificados no título III, capítulo 3, do presente regulamento;

b)Qualquer referência a um produto nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os sistemas de IA que se enquadrem no âmbito do presente regulamento.

2.A autoridade nacional de controlo deve comunicar regularmente à Comissão os resultados das atividades de fiscalização do mercado pertinentes. A autoridade nacional de controlo deve comunicar, sem demora, à Comissão e às autoridades nacionais da concorrência adequadas quaisquer informações reveladas no decurso de atividades de fiscalização do mercado que possam ter interesse para efeitos de aplicação do direito da União relativo às regras de concorrência.

3.No caso dos sistemas de IA de risco elevado relacionados com produtos aos quais se apliquem atos jurídicos enunciados no anexo II, secção A, a autoridade de fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade responsável pelas atividades de fiscalização do mercado designada nos termos desses atos jurídicos.

4.No caso dos sistemas de IA colocados no mercado, colocados em serviço ou utilizados por instituições financeiras regulamentadas pela legislação da União em matéria de serviços financeiros, a autoridade de fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade responsável pela supervisão financeira dessas instituições ao abrigo da referida legislação.

5.No respeitante aos sistemas de IA enumerados no anexo III, ponto 1, alínea a), contanto que sejam utilizados para efeitos de manutenção da ordem pública, e pontos 6 e 7, os Estados-Membros devem designar como autoridades de fiscalização do mercado para efeitos do presente regulamento as autoridades de controlo no domínio da proteção de dados, designadas nos termos da Diretiva (UE) 2016/680 ou do Regulamento (UE) 2016/679, ou as autoridades nacionais competentes que fiscalizam as atividades das autoridades competentes

em matéria de manutenção da ordem pública, imigração ou asilo que colocam em serviço ou utilizam esses sistemas.
6.Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade de fiscalização do mercado dos mesmos.
7.Os Estados-Membros devem facilitar a coordenação entre as autoridades de fiscalização do mercado designadas nos termos do presente regulamento e outras autoridades ou organismos nacionais competentes que supervisionam a aplicação da legislação de harmonização da União enunciada no anexo III ou de outra legislação da União que possa ser aplicável aos sistemas de IA de risco elevado referidos no anexo III.

Artigo 64.º

Acesso a dados e a documentação

1.No que toca ao acesso a dados e a documentação no contexto das suas atividades, as autoridades de fiscalização do mercado devem dispor de total acesso aos conjuntos de dados de treino, validação e teste utilizados pelo fornecedor, incluindo através de interfaces de programação de aplicações ou outros meios e ferramentas técnicas adequadas que possibilitem o acesso remoto.
2.Sempre que necessário para avaliar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no título III, capítulo 2, e mediante pedido fundamentado, deve ser concedido às autoridades de fiscalização do mercado o acesso ao código-fonte do sistema de IA.
3.As autoridades ou organismos públicos nacionais que supervisionam ou asseguram, no atinente à utilização de sistemas de IA de risco elevado referidos no anexo III, o respeito das obrigações previstas na legislação da União que protege os direitos fundamentais devem ter poderes para solicitar e aceder a toda a documentação elaborada ou mantida nos termos do presente regulamento, nos casos em que o acesso a essa documentação for necessário para o exercício das competências incluídas nos seus mandatos e dentro dos limites das respetivas jurisdições. A autoridade ou o organismo público competente deve informar a autoridade de fiscalização do mercado do Estado-Membro em causa de qualquer pedido dessa natureza.
4.No prazo de três meses a contar da entrada em vigor do presente regulamento, cada Estado-Membro deve identificar as autoridades ou os organismos públicos referidos no n.º 3 e elaborar uma lista que esteja acessível ao público no sítio Web da autoridade nacional de controlo. Os Estados-Membros devem notificar a lista à Comissão e a todos os outros Estados-Membros e mantê-la atualizada.
5.Se a documentação referida no n.º 3 for insuficiente para determinar se ocorreu um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais, a autoridade ou o organismo público referido no n.º 3 pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado para organizar a testagem do sistema de IA de risco elevado por recurso a meios técnicos. A autoridade de fiscalização do mercado deve organizar a testagem com a participação ativa da autoridade ou do organismo público requerente num prazo razoável após o pedido.
6.Todas as informações e documentação que as autoridades ou organismos públicos nacionais referidos no n.º 3 obtenham nos termos das disposições do presente artigo devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 70.º.

Artigo 65.º
Procedimento aplicável aos sistemas de inteligência artificial que apresentam riscos a nível nacional

1.Entende-se por «sistema de IA que apresenta um risco» um «produto que apresenta um risco», na aceção do artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, contanto que estejam em causa riscos para a saúde e a segurança ou para a proteção dos direitos fundamentais das pessoas.

2.Se a autoridade de fiscalização do mercado de um Estado-Membro tiver motivos suficientes para considerar que um sistema de IA apresenta um risco, tal como descrito no n.º 1, deve avaliar o sistema de IA em causa no que diz respeito à conformidade do mesmo com todos os requisitos e obrigações previstos no presente regulamento. Se estiverem presentes riscos para a proteção dos direitos fundamentais, a autoridade de fiscalização do mercado também deve informar as autoridades ou os organismos públicos nacionais competentes referidos no artigo 64.º, n.º 3. Os operadores envolvidos devem cooperar na medida do necessário com as autoridades de fiscalização do mercado e as outras autoridades ou organismos públicos nacionais referidos no artigo 64.º, n.º 3.

Se, no decurso dessa avaliação, a autoridade de fiscalização do mercado verificar que o sistema de IA não cumpre os requisitos e as obrigações previstas no presente regulamento, deve exigir imediatamente ao operador correspondente que tome todas as medidas corretivas adequadas para assegurar a conformidade do sistema de IA, para o retirar do mercado ou para o recolher num prazo fixado pela autoridade que seja razoável e proporcionado à natureza do risco.

A autoridade de fiscalização do mercado deve informar desse facto o organismo notificado pertinente. O artigo 18.º do Regulamento (UE) 2019/1020 é aplicável às medidas referidas no segundo parágrafo.

3.Se a autoridade de fiscalização do mercado considerar que a não conformidade não se limita ao respetivo território nacional, deve comunicar à Comissão e aos outros Estados-Membros os resultados da avaliação e as medidas que exigiu que o operador tomasse.

4.O operador deve garantir a aplicação de todas as medidas corretivas adequadas relativamente aos sistemas de IA em causa por si disponibilizados no mercado da União.

5.Se o operador de um sistema de IA não adotar as medidas corretivas adequadas no prazo referido no n.º 2, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a disponibilização do sistema de IA no respetivo mercado nacional, para o retirar do mercado ou para o recolher. A referida autoridade deve informar sem demora a Comissão e os outros Estados-Membros da adoção de tais medidas.

6.A notificação referida no n.º 5 deve conter todas as informações disponíveis, em especial os dados necessários à identificação do sistema de IA não conforme, a origem do sistema de IA, a natureza da alegada não conformidade e o risco conexo, a natureza e a duração das medidas nacionais adotadas, bem como as observações do operador em causa. As autoridades de fiscalização do mercado devem, nomeadamente, indicar se a não conformidade se deve a uma ou várias das seguintes razões:

a)O incumprimento, por parte do sistema de IA, dos requisitos estabelecidos no título III, capítulo 2;

b)Deficiências das normas harmonizadas ou das especificações comuns que, nos termos dos artigos 40.º e 41.º, conferem uma presunção de conformidade.

7.As autoridades de fiscalização do mercado dos Estados-Membros, com exceção da autoridade de fiscalização do mercado do Estado-Membro que desencadeou o procedimento, devem informar sem demora a Comissão e os outros Estados-Membros das medidas tomadas e das informações adicionais de que disponham relativamente à não conformidade do sistema de IA em causa e, em caso de desacordo com a medida nacional notificada, das suas objeções.

8.Se, no prazo de três meses a contar da receção das informações referidas no n.º 5, nem os Estados-Membros nem a Comissão tiverem levantado objeções à medida provisória tomada por um Estado-Membro, considera-se que a mesma é justificada. Esta disposição aplica-se sem prejuízo dos direitos processuais do operador em causa previstos no artigo 18.º do Regulamento (UE) 2019/1020.

9.As autoridades de fiscalização do mercado de todos os Estados-Membros devem garantir que as medidas restritivas adequadas relativas ao produto em causa, como a retirada deste do respetivo mercado, sejam tomadas sem demora.

Artigo 66.º

Procedimento de salvaguarda da União

1.Se, nos três meses subsequentes à receção da notificação a que se refere o artigo 65.º, n.º 5, um Estado-Membro levantar objeções a uma medida tomada por outro Estado-Membro, ou a Comissão considerar que a medida é contrária ao direito da União, a Comissão procede sem demora a consultas com o Estado-Membro e o operador ou operadores em causa e avalia a medida nacional. Em função dos resultados dessa avaliação, a Comissão decide se a medida nacional é ou não justificada no prazo de nove meses a contar da notificação referida no artigo 65.º, n.º 5, e notifica essa decisão ao Estado-Membro em causa.

2.Se a medida nacional for considerada justificada, todos os Estados-Membros devem tomar as medidas necessárias para garantir que o sistema de IA não conforme seja retirado dos respetivos mercados, informando a Comissão das mesmas. Se a medida nacional for considerada injustificada, o Estado-Membro em causa deve revogá-la.

3.Se a medida nacional for considerada justificada e a não conformidade do sistema de IA for atribuída a deficiências das normas harmonizadas ou das especificações comuns referidas nos artigos 40.º e 41.º do presente regulamento, a Comissão aplica o procedimento previsto no artigo 11.º do Regulamento (UE) n.º 1025/2012.

Artigo 67.º

Sistemas de inteligência artificial conformes que apresentam um risco

1.Se, uma vez realizada a avaliação prevista no artigo 65.º, a autoridade de fiscalização do mercado de um Estado-Membro verificar que, embora conforme com o presente regulamento, um sistema de IA apresenta um risco para a saúde ou a segurança das pessoas, para o cumprimento de obrigações impostas por legislação da União ou nacional destinada a proteger os direitos fundamentais ou para outras vertentes de proteção do interesse público, deve exigir ao operador correspondente que tome todas as medidas adequadas para garantir que quando o sistema de IA em causa for colocado no mercado ou colocado em serviço já não apresente esse risco, para o retirar do mercado ou para o recolher num prazo fixado pela autoridade que seja razoável e proporcionado à natureza do risco.

2.O fornecedor ou outros operadores envolvidos devem assegurar que a medida corretiva seja tomada no tocante a todos os sistemas de IA em causa que tenham disponibilizado no mercado da União no prazo fixado pela autoridade de fiscalização do mercado do Estado-Membro referido no n.º 1.
3.O Estado-Membro deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto. Essa notificação deve incluir todas as informações disponíveis, em particular os dados necessários à identificação do sistema de IA em causa, a origem e a cadeia de abastecimento do sistema de IA, a natureza do risco conexo e a natureza e duração das medidas nacionais adotadas.
4.A Comissão procede sem demora a consultas com os Estados-Membros e com o operador em causa e avalia as medidas nacionais adotadas. Em função dos resultados dessa avaliação, a Comissão decide se a medida é ou não justificada e, se necessário, propõe medidas adequadas.
5.A Comissão designa os Estados-Membros como destinatários da decisão.

Artigo 68.º
Não conformidade formal

1.Se a autoridade de fiscalização do mercado de um Estado-Membro constatar um dos factos a seguir enunciados, deve exigir ao fornecedor em causa que ponha termo à não conformidade verificada:

a)A marcação de conformidade foi aposta em violação do disposto no artigo 49.º;

b)A marcação de conformidade não foi aposta;

c)A declaração de conformidade UE não foi elaborada;

d)A declaração de conformidade UE não foi elaborada corretamente;

e)O número de identificação do organismo notificado envolvido, se for caso disso, no procedimento de avaliação da conformidade não foi aposto.

2.Se a não conformidade referida no n.º 1 persistir, o Estado-Membro em causa deve tomar as medidas adequadas para restringir ou proibir a disponibilização no mercado do sistema de IA de risco elevado ou para garantir que o mesmo seja recolhido ou retirado do mercado.

TÍTULO IX
CÓDIGOS DE CONDUTA

Artigo 69.º
Códigos de conduta

1.A Comissão e os Estados-Membros devem incentivar e facilitar a elaboração de códigos de conduta destinados a fomentar a aplicação voluntária dos requisitos estabelecidos no título III, capítulo 2, a sistemas de IA que não sejam sistemas de IA de risco elevado, com base em especificações técnicas e soluções que configurem meios adequados de assegurar a conformidade com os referidos requisitos atendendo à finalidade prevista dos sistemas.
2.A Comissão e o Comité devem incentivar e facilitar a elaboração de códigos de conduta destinados a fomentar a aplicação voluntária a sistemas de IA de requisitos relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento, com base em objetivos claros e indicadores-chave de desempenho que permitam medir a consecução desses objetivos.

3.Os códigos de conduta podem ser elaborados por fornecedores de sistemas de IA a título individual ou por organizações que os representem, ou ambos, nomeadamente com a participação de utilizadores e de quaisquer partes interessadas e das respetivas organizações representativas. Os códigos de conduta podem abranger um ou mais sistemas de IA, tendo em conta a semelhança da finalidade prevista desses sistemas.
4.A Comissão e o Comité devem ter em conta as necessidades e os interesses específicos dos fornecedores de pequena dimensão e das empresas em fase de arranque quando incentivam e facilitam a elaboração de códigos de conduta.

TÍTULO X
CONFIDENCIALIDADE E SANÇÕES

Artigo 70.º
Confidencialidade

1.As autoridades nacionais competentes e os organismos notificados envolvidos na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades de modo que protejam, em especial:

a)Os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte, exceto nos casos a que se refere o artigo 5.º da Diretiva 2016/943 relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais;

b)A execução efetiva do presente regulamento, em especial no que diz respeito à realização de inspeções, investigações ou auditorias; c) Interesses públicos e nacionais em matéria de segurança;

c)A integridade de processos penais ou administrativos.

2.Sem prejuízo do n.º 1, no caso de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, utilizados por autoridades competentes em matéria de manutenção da ordem pública, de imigração ou de asilo, as informações trocadas numa base confidencial entre as autoridades nacionais competentes e entre as autoridades nacionais competentes e a Comissão não podem ser divulgadas sem consultar previamente a autoridade nacional competente de origem e o utilizador, quando tal divulgação prejudicar interesses públicos e nacionais em matéria de segurança.
Se as autoridades competentes em matéria de manutenção da ordem pública, de imigração ou de asilo forem os fornecedores de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, a documentação técnica referida no anexo IV deve permanecer nas instalações dessas autoridades. As referidas autoridades devem assegurar que as autoridades de fiscalização do mercado referidas no artigo 63.º, n.os 5 e 6, consoante o caso, possam, mediante pedido, aceder imediatamente à documentação ou obter uma cópia da mesma. O acesso à referida documentação ou a qualquer cópia da mesma só pode ser concedido ao pessoal da autoridade de fiscalização do mercado que detenha o nível apropriado de credenciação de segurança.
3.O disposto nos n.os 1 e 2 não afeta os direitos e obrigações da Comissão, dos Estados-Membros e dos organismos notificados no que se refere ao intercâmbio de informações e à divulgação de avisos, nem o dever de informação que incumbe às partes em causa no âmbito do direito penal dos Estados-Membros.

4.A Comissão e os Estados-Membros podem, quando necessário, trocar informações confidenciais com autoridades reguladoras de países terceiros com as quais tenham celebrado acordos de confidencialidade bilaterais ou multilaterais desde que garantam um nível adequado de confidencialidade.

Artigo 71.º

Sanções

1.Em conformidade com os termos e as condições previstas no presente regulamento, os Estados-Membros devem estabelecer o regime de sanções, incluindo coimas, aplicáveis em caso de infração ao presente regulamento e devem tomar todas as medidas necessárias para garantir que o mesmo é aplicado correta e eficazmente. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Devem ter especialmente em conta os interesses dos fornecedores de pequena dimensão e das empresas em fase de arranque e a respetiva viabilidade económica.

2.Os Estados-Membros devem notificar a Comissão dessas regras e dessas medidas e também, sem demora, de qualquer alteração ulterior das mesmas.

3.Ficam sujeitas a coimas até 30 000 000 EUR ou, se o infrator for uma empresa, até 6 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado, as seguintes infrações:

a)Incumprimento da proibição das práticas de inteligência artificial referidas no artigo 5.º;

b)Não conformidade do sistema de IA com os requisitos estabelecidos no artigo 10.º.

4.A não conformidade do sistema de IA com quaisquer requisitos ou obrigações por força do presente regulamento, que não os estabelecidos nos artigos 5.º e 10.º, fica sujeita a coimas até 20 000 000 EUR ou, se o infrator for uma empresa, até 4 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado.

5.O fornecimento de informações incorretas, incompletas ou enganadoras aos organismos notificados e às autoridades nacionais competentes em resposta a um pedido fica sujeito a coimas até 10 000 000 EUR ou, se o infrator for uma empresa, até 2 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado.

6.A decisão relativa ao montante da coima a aplicar em cada caso deve ter em conta todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

a)A natureza, a gravidade e a duração da infração e das suas consequências;

b)Se outras autoridades de fiscalização do mercado já aplicaram coimas ao mesmo operador pela mesma infração;

c)A dimensão e quota-parte de mercado do operador que cometeu a infração.

7.Cada Estado-Membro deve definir regras que permitam determinar se e em que medida podem ser aplicadas coimas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.

8.Dependendo do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de maneira que as coimas sejam impostas por tribunais nacionais ou por outros organismos competentes, tal como previsto nesses Estados-Membros. A aplicação dessas regras nesses Estados-Membros deve ter um efeito equivalente.

Artigo 72.º

Coimas aplicáveis às instituições, órgãos e organismos da União

1.A Autoridade Europeia para a Proteção de Dados pode impor coimas às instituições, órgãos e organismos da União que se enquadrem no âmbito do presente regulamento. Ao decidir sobre a imposição de uma coima e o montante da mesma, devem ser tidas em conta, em cada caso, todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

a)A natureza, a gravidade e a duração da infração e das suas consequências;

b)A cooperação com a Autoridade Europeia para a Proteção de Dados no sentido de corrigir a infração e atenuar os possíveis efeitos adversos da mesma, nomeadamente o cumprimento de eventuais medidas previamente impostas pela Autoridade Europeia para a Proteção de Dados contra a instituição, órgão ou organismo da União em causa relativamente à mesma matéria;

c)Quaisquer infrações similares anteriormente cometidas pela instituição, órgão ou organismo da União.

2.Ficam sujeitas a coimas até 500 000 EUR as seguintes infrações:

a)Incumprimento da proibição das práticas de inteligência artificial referidas no artigo 5.º;

b)Não conformidade do sistema de IA com os requisitos estabelecidos no artigo 10.º.

3.A não conformidade do sistema de IA com quaisquer requisitos ou obrigações por força do presente regulamento, que não os estabelecidos nos artigos 5.º e 10.º, fica sujeita a coimas até 250 000 EUR.

4.Antes de tomar decisões nos termos do presente artigo, a Autoridade Europeia para a Proteção de Dados deve conceder à instituição, órgão ou organismo da União objeto do procedimento por si aplicado a oportunidade de se pronunciar sobre a matéria que constitui possível infração. A Autoridade Europeia para a Proteção de Dados deve basear as suas decisões unicamente nos elementos e nas circunstâncias relativamente às quais as partes em causa puderam apresentar as observações. Os queixosos, caso existam, devem ser estreitamente associados ao procedimento.

5.Os direitos de defesa das partes em causa devem ser plenamente respeitados no desenrolar do processo. As partes interessadas devem ter o direito de aceder ao processo da Autoridade Europeia para a Proteção de Dados, sob reserva do interesse legítimo dos indivíduos ou das empresas relativamente à proteção dos respetivos dados pessoais ou segredos comerciais.

6.Os fundos recolhidos em resultado da imposição das coimas previstas no presente artigo constituem receitas do orçamento geral da União.

TÍTULO XI
DELEGAÇÃO DE PODERES E PROCEDIMENTO DE COMITÉ

Artigo 73.º

Exercício da delegação

1.O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2.O poder de adotar atos delegados referido no artigo 4.º, no artigo 7.º, n.º 1, no artigo 11.º, n.º 3, no artigo 43.º, n.os 5 e 6, e no artigo 48.º, n.º 5, é conferido à

Comissão por tempo indeterminado contar de [data de entrada em vigor do presente regulamento].

3.A delegação de poderes referida no artigo 4.º, no artigo 7.º, n.º 1, no artigo 11.º, n.º 3, no artigo 43.º, n.os 5 e 6, e no artigo 48.º, n.º 5, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no Jornal Oficial da União Europeia ou numa data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4.Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

5.Os atos delegados adotados nos termos do artigo 4.º, do artigo 7.º, n.º 1, do artigo 11.º, n.º 3, do artigo 43.º, n.os 5 e 6, e do artigo 48.º, n.º 5, só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de três meses a contar da notificação desses atos a estas duas instituições ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 74.º

Procedimento de comité

1.A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2.Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

TÍTULO XII
DISPOSIÇÕES FINAIS

Artigo 75.º

Alteração do Regulamento (CE) n.º 300/2008

Ao artigo 4.º, n.º 3, do Regulamento (CE) n.º 300/2008, é aditado o seguinte parágrafo:

«Aquando da adoção de medidas de execução relacionadas com especificações técnicas e procedimentos para a aprovação e utilização de equipamentos de segurança respeitantes a sistemas de inteligência artificial na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 76.º

Alteração do Regulamento (UE) n.º 167/2013

Ao artigo 17.º, n.º 5, do Regulamento (UE) n.º 167/2013, é aditado o seguinte parágrafo:

«Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 77.º

Alteração do Regulamento (UE) n.º 168/2013

Ao artigo 22.º, n.º 5, do Regulamento (UE) n.º 168/2013, é aditado o seguinte parágrafo:
«Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 78.º

Alteração da Diretiva 2014/90/UE

Ao artigo 8.º da Diretiva 2014/90/UE, é aditado o seguinte número:
«4. Aquando da realização das atividades previstas no n.º 1 e da adoção de especificações técnicas e normas de ensaio em conformidade com os n.os 2 e 3 respeitantes a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, Comissão tem em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 79.º

Alteração da Diretiva (UE) 2016/797

Ao artigo 5.º da Diretiva (UE) 2016/797, é aditado o seguinte número:
«12. «Aquando da adoção de atos delegados nos termos do n.º 1 e de atos de execução nos termos do n.º 11 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 80.º

Alteração do Regulamento (UE) 2018/858

Ao artigo 5.º do Regulamento (UE) 2018/858, é aditado o seguinte número:
«4. Aquando da adoção de atos delegados nos termos do n.º 3 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 81.º

Alteração do Regulamento (UE) 2018/1139

O Regulamento (UE) 2018/1139 é alterado do seguinte modo:
1) Ao artigo 17.º, é aditado o seguinte número:
«3. Sem prejuízo do disposto no n.º 2, aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»;

2) Ao artigo 19.º, é aditado o seguinte número:
«4. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;
3) Ao artigo 43.º, é aditado o seguinte número:
«4. Aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;
4) Ao artigo 47.º, é aditado o seguinte número:
«3. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;
5) Ao artigo 57.º, é aditado o seguinte parágrafo:
Aquando da adoção desses atos de execução relativamente a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;
6) Ao artigo 58.º, é aditado o seguinte número:
«3. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»

Artigo 82.º

Alteração do Regulamento (UE) 2019/2144

Ao artigo 11.º do Regulamento (UE) 2019/2144, é aditado o seguinte número:
«3. Aquando da adoção de atos de execução nos termos do n.º 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 83.º

Sistemas de inteligência artificial já colocados no mercado ou em serviço

1.O presente regulamento não se aplica aos sistemas de IA que sejam componentes dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX que tenham sido colocados no mercado ou colocados em serviço antes de [12 meses após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2], salvo se a substituição ou alteração desses atos jurídicos implicar uma alteração significativa da conceção ou da finalidade prevista do sistema ou dos sistemas de IA em causa.

Os requisitos estabelecidos no presente regulamento devem ser tidos em conta, se for caso disso, na avaliação de cada um dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX, a realizar como previsto nos respetivos atos.

2.O presente regulamento só se aplica aos sistemas de IA de risco elevado, que não os referidos no n.º 1, que tenham sido colocados no mercado ou colocados

em serviço antes de [data de aplicação do presente regulamento referida no artigo 85.º, n.º 2], se, após esta data, os referidos sistemas forem sido sujeitos a alterações significativas em termos de conceção ou finalidade prevista.

Artigo 84.º

Avaliação e reexame

1.A Comissão avalia a necessidade de alterar a lista que consta do anexo III uma vez por ano após a entrada em vigor do presente regulamento.

2.Até [três anos após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2] e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e reexame do presente regulamento. Os relatórios devem ser divulgados ao público.

3.Os relatórios referidos no n.º 2 devem dar especial atenção ao seguinte:

a)A situação das autoridades nacionais competentes em termos dos recursos financeiros e humanos necessários para exercer eficazmente as funções que lhes foram atribuídas nos termos do presente regulamento;

b)O estado das sanções, designadamente das coimas referidas no artigo 71.º, n.º 1, aplicadas pelos Estados-Membros em consequência de infrações às disposições do presente regulamento.

4.No prazo de [três anos a contar da data de aplicação do presente regulamento referida no artigo 85.º, n.º 2] e subsequentemente de quatro em quatro anos, a Comissão avalia o impacto e a eficácia dos códigos de conduta com vista a fomentar a aplicação dos requisitos estabelecidos no título III, capítulo 2, e, eventualmente, de outros requisitos adicionais a sistemas de IA que não sejam sistemas de IA de risco elevado.

5.Para efeitos do disposto nos n.os 1 a 4, o Comité, os Estados-Membros e as autoridades nacionais competentes devem facultar à Comissão as informações que esta solicitar.

6.Ao efetuar as avaliações e os reexames a que se referem os n.os 1 a 4, a Comissão tem em consideração as posições e as conclusões do Comité, do Parlamento Europeu, do Conselho e de outros organismos ou fontes pertinentes.

7.Se necessário, a Comissão apresenta propostas adequadas com vista a alterar o presente regulamento, atendendo, em especial, à evolução das tecnologias e aos progressos da sociedade da informação.

Artigo 85.º

Entrada em vigor e aplicação

1.O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

2.O presente regulamento é aplicável a partir de [vinte e quatro meses após a sua entrada em vigor].

3.Em derrogação do disposto no n.º 2:

a)O título III, capítulo 4, e o título VI são aplicáveis a partir de [três meses após a entrada em vigor do presente regulamento];

b)O artigo 71.º é aplicável a partir de [doze meses após a entrada em vigor do presente regulamento].

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.
Feito em Bruxelas, em

Pelo Parlamento Europeu Pelo Conselho O Presidente O Presidente

FICHA FINANCEIRA LEGISLATIVA

1.CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangido(s)

1.3. A proposta/iniciativa refere-se a:

1.4. Objetivo(s)

1.4.1.Objetivo(s) geral(ais)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e impacto esperados

1.4.4. Indicadores de resultados

1.5. Justificação da proposta/iniciativa

1.5.1.Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa

1.5.2. Valor acrescentado da participação da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados

1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação

1.6. Duração e impacto financeiro da proposta/iniciativa

1.7. Modalidade(s) de gestão prevista(s)

2.MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema de gestão e de controlo

2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos

2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar

2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)

2.3.Medidas de prevenção de fraudes e irregularidades

3.IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1.Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

3.2.Impacto financeiro estimado da proposta nas dotações

3.2.1.Síntese do impacto estimado nas dotações operacionais

3.2.2.Estimativa das realizações financiadas com dotações operacionais

3.2.3. Síntese do impacto estimado nas dotações de natureza administrativa

3.2.4.Compatibilidade com o atual quadro financeiro plurianual

3.2.5.Participação de terceiros no financiamento

3.3.Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1.CONTEXTO DA PROPOSTA/INICIATIVA

1.1.Denominação da proposta/iniciativa

Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União

1.2.Domínio(s) de intervenção abrangido(s)

Redes de Comunicação, Conteúdos e Tecnologias;
Mercado interno, Indústria, Empreendedorismo e PME;
O impacto orçamental diz respeito às novas atribuições confiadas à Comissão, incluindo o apoio ao Comité Europeu para a Inteligência Artificial;
Atividade: construir o futuro digital da Europa.

1.3.A proposta/iniciativa refere-se a:

X uma nova ação
□ uma nova ação na sequência de um projeto-piloto/ação preparatória 64
□ uma prorrogação de uma ação existente
□ uma ação redirecionada para uma nova ação

1.4.Objetivo(s)

1.4.1.Objetivo(s) geral(ais)

O objetivo geral da intervenção consiste em assegurar o correto funcionamento do mercado único, criando condições para o desenvolvimento e a utilização de uma inteligência artificial de confiança na União.

1.4.2.Objetivo(s) específico(s)

Objetivo específico n.º 1
Definir requisitos específicos aplicáveis aos sistemas de IA e estabelecer obrigações para todos os participantes da cadeia de valor com vista a assegurar que os sistemas de IA colocados no mercado e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União;
Objetivo específico n.º 2
Garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA, clarificando quais requisitos essenciais, obrigações e

procedimentos relativos à conformidade e ao cumprimento devem ser seguidos para colocar ou utilizar um sistema de IA no mercado da União;
Objetivo específico n.º 3
Reforçar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA, conferindo novos poderes às autoridades competentes, atribuindo-lhes recursos e definindo novas regras relativas aos procedimentos de avaliação da conformidade e de acompanhamento ex post, bem como à divisão das funções de governação e supervisão entre os níveis nacional e da UE;
Objetivo específico n.º 4
Facilitar o desenvolvimento de um mercado único para aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado, atuando a nível da UE para definir requisitos mínimos aplicáveis aos sistemas de IA que serão colocados e utilizados no mercado da União em conformidade com a legislação em vigor em matéria de direitos fundamentais e segurança.

1.4.3.Resultado(s) e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada.
Os fornecedores de IA devem beneficiar de um conjunto de requisitos mínimos, mas claros, que criem segurança jurídica e garantam o acesso a todo o mercado único.
Os utilizadores de IA devem beneficiar da segurança jurídica de que os sistemas de IA de risco elevado que compram cumprem a legislação e os valores europeus.
Os consumidores devem beneficiar da redução do risco de violações da sua segurança e dos seus direitos fundamentais.

1.4.4.Indicadores de resultados

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.
Indicador 1
Número de incidentes graves ou desempenhos de inteligência artificial que constituem um incidente grave ou uma infração às obrigações em matéria de direitos fundamentais (semestral) por áreas de aplicações e calculado: a) em termos absolutos, b) como percentagem das aplicações implantadas; c) como percentagem dos cidadãos envolvidos.
Indicador 2
a) Investimento total em IA na UE (anual)
b) Investimento total em IA por Estado-Membro (anual)
c) Percentagem de empresas que utilizam IA (anual)
d) Percentagem de PME que utilizam IA (anual)
As alíneas a) e b) serão calculadas com base em fontes oficiais, usando como valores de referência estimativas privadas
c) Os dados referentes às alíneas c) e d) serão recolhidos por meio de inquéritos regulares junto das empresas

1.5.Justificação da proposta/iniciativa

1.5.1.Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa

O regulamento deve ser plenamente aplicável um ano e meio após a sua adoção. Contudo, antes dessa data devem já estar em funcionamento elementos da estrutura de governação. Em especial, os Estados-Membros devem ter

previamente designado autoridades existentes e/ou criado novas autoridades para a execução das funções definidas na legislação, sendo que o Comité Europeu para a Inteligência Artificial deve estar criado e em funcionamento. A base de dados europeia de sistemas de IA deve estar a funcionar em pleno à data de aplicação do regulamento. Assim, paralelamente ao processo de adoção, torna-se necessário criar a base de dados, para que o seu desenvolvimento esteja concluído quando o regulamento entrar em vigor.

> *1.5.2.Valor acrescentado da participação da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.*

A emergência de um mosaico de regras nacionais potencialmente divergentes prejudicará o fornecimento homogéneo de sistemas de IA em toda a UE e será ineficaz para garantir a segurança e a proteção dos direitos fundamentais e dos valores da União nos diferentes Estados-Membros. Uma ação legislativa comum no domínio da IA a nível da UE pode estimular o mercado interno e revela grande potencial para proporcionar à indústria europeia uma vantagem competitiva a nível global e economias de escala que não podem ser conseguidas pelos Estados-Membros de forma isolada.

> *1.5.3.Ensinamentos retirados de experiências anteriores semelhantes*

A Diretiva Comércio Eletrónico (Diretiva 2000/31/CE) estabelece o quadro central para o funcionamento do mercado único e a supervisão dos serviços digitais e define uma estrutura de base para um mecanismo de cooperação geral entre os Estados-Membros, abrangendo, em princípio, todos os requisitos aplicáveis aos serviços digitais. A avaliação da diretiva evidenciou insuficiências em vários aspetos deste mecanismo de cooperação, incluindo aspetos processuais importantes, como a ausência de prazos claros para as respostas dos Estados-Membros, juntamente com uma ausência geral de respostas aos pedidos dirigidos pelas suas contrapartes. Tal conduziu, ao longo dos anos, a uma falta de confiança entre os Estados-Membros na resposta a preocupações sobre os fornecedores que oferecem serviços digitais transfronteiras. A avaliação da diretiva mostrou a necessidade de definir um conjunto de regras e requisitos diferenciados a nível europeu. Por este motivo, a aplicação das obrigações específicas estabelecidas no presente regulamento exigirá um mecanismo de cooperação específico a nível da UE, com uma estrutura de governação que assegure a coordenação de organismos responsáveis específicos a nível da UE.

> *1.5.4.Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados*

O regulamento que estabelece regras harmonizadas em matéria de inteligência artificial e altera determinados atos legislativos da União define um novo quadro comum de requisitos aplicáveis aos sistemas de IA, que vai além do enquadramento previsto na legislação existente. Por este motivo, esta proposta obriga ao estabelecimento de uma nova função reguladora e coordenadora a nível nacional e europeu.

No que diz respeito a possíveis sinergias com outros instrumentos adequados, o papel das autoridades notificadoras a nível nacional pode ser desempenhado

pelas autoridades nacionais responsáveis pelo exercício de funções semelhantes nos termos de outros regulamentos da UE.

Além disso, o aumento da confiança na IA e o subsequente incentivo ao investimento no desenvolvimento e na adoção de soluções de IA contribuirão para os objetivos do Programa Europa Digital (PED), que define a difusão da IA como uma das suas cinco prioridades.

1.5.5.Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação

Haverá lugar à reafetação de pessoal. Os restantes custos serão suportados pela dotação do PED, atendendo a que o objetivo do presente regulamento — garantir uma IA de confiança — contribui diretamente para um dos principais objetivos do programa — acelerar o desenvolvimento e a implantação da IA na Europa.

1.6.Duração e impacto financeiro da proposta/iniciativa

☐ duração limitada

–☐ em vigor entre [DD/MM]AAAA e [DD/MM]AAAA

–☐ Impacto financeiro no período compreendido entre AAAA e AAAA para as dotações de autorização e entre AAAA a AAAA para as dotações de pagamento.

X duração ilimitada

–Aplicação com um período de arranque progressivo entre um/dois anos (a determinar),

–seguido de um período de aplicação a um ritmo de cruzeiro.

1.7.Modalidade(s) de gestão prevista(s) 65

X Gestão direta por parte da Comissão

–☐ pelos seus serviços, incluindo o pessoal nas delegações da União;

–☐ pelas agências de execução

☐ Gestão partilhada com os Estados-Membros

☐ Gestão indireta confiando tarefas de execução orçamental:

–☐ a países terceiros ou organismos por estes designados;

–☐ a organizações internacionais e respetivas agências (a especificar);

–☐ ao BEI e ao Fundo Europeu de Investimento;

–☐ aos organismos referidos nos artigos 70.º e 71.º do Regulamento Financeiro;

–☐ a organismos de direito público;

–☐ aos organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;

–☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

–☐ a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

–Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».

Observações

2.MEDIDAS DE GESTÃO

2.1.Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições.

O regulamento será reexaminado e avaliado no prazo de cinco anos a contar da data de entrada em vigor. A Comissão apresentará um relatório sobre as conclusões da avaliação ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu.

2.2.Sistema(s) de gestão e de controlo

2.2.1.Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos

O regulamento estabelece uma nova política no que respeita a regras harmonizadas para o fornecimento de sistemas de inteligência artificial no mercado interno, assegurando simultaneamente o respeito da segurança e dos direitos fundamentais. Estas novas regras exigem um mecanismo de controlo da coerência na aplicação transfronteiras das obrigações do presente regulamento, sob a forma de um novo grupo consultivo que coordene as atividades das autoridades nacionais.

Para desempenhar estas novas funções, é necessário dotar os serviços da Comissão dos recursos adequados. Estima-se que a aplicação do novo regulamento exija 10 ETC (5 ETC para apoiar as atividades do Comité e 5 ETC para a Autoridade Europeia para a Proteção de Dados na qualidade de organismo notificador para os sistemas de IA implantados por um organismo da União Europeia).

2.2.2.Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar

Para garantir que os membros do Comité tenham a possibilidade de fazer uma análise informada com base em provas factuais, prevê-se que o Comité seja apoiado pela estrutura administrativa da Comissão e que seja criado um grupo de peritos para prestar informações especializadas adicionais, se for caso disso.

2.2.3.Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)

Em relação às despesas de reunião, atendendo ao baixo valor por transação (por exemplo, reembolso das despesas de viagem por reunião), os procedimentos de controlo habituais afiguram-se suficientes. Relativamente ao desenvolvimento da base de dados, a atribuição de contratos é abrangida pelo forte sistema de controlo interno existente na DG CNECT, baseado em atividades de contratação centralizadas.

2.3.Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas, como, por exemplo, da estratégia antifraude.

As atuais medidas de prevenção da fraude aplicáveis à Comissão cobrirão as dotações adicionais necessárias para efeitos do presente regulamento.

3.IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1.Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

·Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

RUBRICA DO QUADRO FINANCEIRO PLURIANUAL	RUBRICA ORÇAMENTAL	TIPO DE DESPESA	PARTICIPAÇÃO			
	Número	DD/DND 66	Dos Países EFTA 67	Dos Países Candidatos 68	De Países Terceiros	Na Aceção do Artigo 21.º, n.º 2, Alínea b), do Regulamento Financeiro
7	20 02 06 Despesas administrativas	DND	Não	Não	Não	Não
1	02 04 03 PED — Inteligência Artificial	DD	Sim	Não	Não	Não
1	02 01 30 01 Despesas de apoio ao Programa Europa Digital	DND	Sim	Não	Não	Não

3.2.Impacto financeiro estimado da proposta nas dotações

3.2.1.Síntese do impacto estimado na despesa nas dotações operacionais

–☐ A proposta/iniciativa não acarreta a utilização de dotações operacionais

–X A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

RUBRICA DO QUADRO FINANCEIRO PLURIANUAL									
DG: CNECT			ANO 2022	ANO 2023	ANO 2024	ANO 2025	ANO 2026	ANO 2027	TOTAL
DOTAÇÕES OPERACIONAIS									
Rubrica Orçamental 70 02 04 03	Autorizações	(1a)		1,000					1,000
	Pagamentos	(2a)		0,600	0,100	0,100	0,100	0,100	1,000
Rubrica Orçamental	Autorizações	(1b)							
	Pagamentos	(2b)							
DOTAÇÕES DE NATUREZA ADMINISTRATIVA FINANCIADAS A PARTIR DA DOTAÇÃO DE PROGRAMAS ESPECÍFICOS 71									
Rubrica Orçamental		(3)		0,240	0,240	0,240	0,240	0,240	1,200
Total das Dotações para a DG CNECT	Autorizações	=1a+1b+3		1,240		0,240	0,240	0,240	2,200
	Pagamentos	=2a+2b+3		0,840	0,340	0,340	0,340	0,340	2,200

Total das Dotações Operacionais	Autorizações	(4)		1,000						1,000
	Pagamentos	(5)		0,600	0,100	0,100	0,100	0,100		1,000
Total das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)		0,240	0,240	0,240	0,240	0,240		1,200
Total das Dotações para a Rubrica 1 do Quadro Financeiro Plurianual	Autorizações	= 4+6		1,240	0,240	0,240	0,240	0,240		2,200
	Pagamentos	=5+6		0,840	0,340	0,340	0,340	0,340		2,200

Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica, repetir a secção acima:

Total das Dotações Operacionais (Todas as Rubricas Operacionais)	Autorizações	(4)								
	Pagamentos	(5)								
Total das Dotações de Natureza Administrativa Financiadas a Partir da Dotação de Programas Específicos (Todas as Rubricas Operacionais)		(6)								
Total das Dotações para as Rubricas 1 a 6 do Quadro Financeiro Plurianual (Montante de Referência)	Autorizações	= 4+6								
	Pagamentos	=5+6								

Rubrica do Quadro Finamceiro Plurianual	7	«Despesas administrativas»

Esta secção deve ser preenchida com «dados orçamentais de natureza administrativa» a inserir em primeiro lugar no anexo da ficha financeira legislativa (anexo V das regras internas), que é carregada no DECIDE para efeitos das consultas interserviços.

Em milhões de EUR (três casas decimais)

				ANO 2023	ANO 2024	ANO 2025	ANO 2026	ANO 2027	APÓS 2027	TOTAL
DG: CNECT										
RECURSOS HUMANOS				0,760	0,760	0,760	0,760	0,760	0,760	3,800
OUTRAS DESPESAS ADMINISTRATIVAS				0,010	0,010	0,010	0,010	0,010	0,010	0,050
Total DG CNECT		Dotações		0,760	0,760	0,760	0,760	0,760	0,760	3,800
Autoridade Europeia para a Proteção de Dados										
RECURSOS HUMANOS				0,760	0,760	0,760	0,760	0,760	0,760	3,800
OUTRAS DESPESAS ADMINISTRATIVAS										
Total DG CNECT		Dotações		0,760	0,760	0,760	0,760	0,760	0,760	3,800
Total das Dotações para a Rubrica 7 do Quadro Financeiro Plurianual		(Total das autorizações = total dos pagamentos)		1,530	1,530	1,530	1,530	1,530	1,530	7,650

Em milhões de EUR (três casas decimais)

		ANO 2022	ANO 2023	ANO 2024	ANO 2025	ANO 2026	ANO 2027		TOTAL
Total das Dotações para as Rubricas 1 a 7 do Quadro Financeiro Plurianual	Autorizações		2,770	1,770	1,770	1,770	1,770		9,850
	Pagamentos		2,370	1,870	1,870	1,870	1,870		9,850

3.2.2.Estimativa das realizações financiadas com dotações operacionais

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os Objetivos e as Realizações			ANO 2022		ANO 2023		ANO 2024		ANO 2025		ANO 2026		ANO 2027		APÓS 2027		TOTAL	
	REALIZAÇÕES																	
	Tipo	Custo Médio	Nº	Custo	Nº	Custo	Nº	Custo	Nº	Custo	Nº	Custo	Nº	Custo	Nº	Custo	Nº Total	Custo Total
Objetivo Específico nº1																		
Base de Dados			1	1,000	1		1		1		1		1		1	0,100	1	1,000
Reuniões - Realização			10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Atividades de Comunicação			2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Subtotal Objetivo Específico nº1																		
Objetivo Específico nº2																		
- Realização																		
Subtotal Objetivo Específico nº2																		
Totais			13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

3.2.3.Síntese do impacto estimado nas dotações de natureza administrativa

–☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

–X A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

	ANO 2022	ANO 2023	ANO 2024	ANO 2025	ANO 2026	ANO 2027	ANO 2027 75	TOTAL
RUBRICA 7 do quadro financeiro plurianual								
Recursos humanos		1,52	1,52	1,52	1,52	1,52	1,52	7,6
Outras despesas administrativas		0,01	0,01	0,01	0,01	0,01	0,01	0,05
Subtotal RUBRICA 7 do quadro financeiro plurianual		1,53	1,53	1,53	1,53	1,53	1,53	7,65
Com exclusão da RUBRICA 7 76 do quadro financeiro plurianual								
Recursos humanos								
Outras despesas de natureza administrativa		0,24	0,24	0,24	0,24	0,24	0,24	1,2
Subtotal com exclusão da RUBRICA 7 do quadro financeiro plurianual		0,24	0,24	0,24	0,24	0,24	0,24	1,2
TOTAL		1,77	1,77	1,77	1,77	1,77	1,77	8,85

As dotações relativas aos recursos humanos e outras despesas administrativas necessárias serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas na DG e, se necessário, pelas eventuais dotações adicionais que sejam concedidas à DG gestora no âmbito do processo de afetação anual e atendendo às restrições orçamentais.

3.2.3.1.Necessidades estimadas de recursos humanos

–□ A proposta/iniciativa não acarreta a utilização de recursos humanos.

–X A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em termos de equivalente a tempo completo

		ANO 2023	ANO 2024	ANO 2025	ANO 2026	ANO 2027	ANO 2027 75	TOTAL
Lugares do quadro do pessoal (funcionários e agentes temporários)								
20 01 02 01 (na sede e nas representações da Comissão)		10	10	10	10	10	10	
20 01 02 03 (nas delegações)								
01 01 01 01 (investigação indireta)								
01 01 01 11 (investigação direta)								
Outras rubricas orçamentais (especificar)								
Pessoal externo (em equivalente a tempo completo: ETC) 78								
20 02 01 (AC, PND e TT da dotação global)								
20 02 03 (AC, AL, PND, TT e JPD nas delegações)								
XX 01 xx yy zz 79	**- na sede**							
	- nas delegações							
01 01 01 02 (AC, PND e TT - Investigação indireta)								
01 01 01 12 (AC, PND e TT - Investigação direta)								
Outras rubricas orçamentais (especificar)								
TOTAL		10	10	10	10	10	10	

XX constitui o domínio de intervenção ou o título orçamental em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais. Espera-se que a AEPD forneça metade dos recursos necessários.

Descricão das tarefas a executar:

Funcionários e agentes temporários	Serão necessários 4 AD ETC e 1 AST ETC incumbidos de preparar um total de 13-16 reuniões, elaborar relatórios, dar seguimento ao trabalho político (por exemplo, relativamente a futuras alterações da lista de aplicações de IA de risco elevado) e manter relações com as autoridades dos Estados-Membros. No caso dos sistemas de IA desenvolvidos pelas instituições da UE, a Autoridade Europeia para a Proteção de Dados é responsável. Com base na experiência acumulada, estima-se que sejam necessários 5 AD ETC para cumprir as responsabilidades da AEPD previstas na proposta legislativa.
Pessoal externo	

3.2.4.Compatibilidade com o atual quadro financeiro plurianual

A proposta/iniciativa:

–X pode ser integralmente financiada por meio da reafetação de fundos no quadro da rubrica pertinente do quadro financeiro plurianual (QFP).

Não é necessário qualquer tipo de reprogramação.

–☐ requer o recurso à margem não afetada na rubrica em causa do QFP e/ou o recurso aos instrumentos especiais definidos no Regulamento QFP.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes, bem como os instrumentos cuja utilização é proposta.

–☐ implica uma revisão do QFP.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes.

3.2.5.Participação de terceiros no financiamento

A proposta/iniciativa:

–X não prevê o cofinanciamento por terceiros

–☐ prevê o seguinte cofinanciamento por terceiros, a seguir estimado:

Dotações em milhões de EUR (três casas decimais)

	Ano N 80	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)			Total
Especificar o organismo de z o organismo de								
TOTAL das dotações cofinanciadas								

3.3.Impacto estimado nas receitas

–☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

–☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

–☐ noutras receitas

–☐ noutras receitas

–indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

RUBRICA ORÇAMENTAL DAS RECEITAS:	DOTAÇÕES DISPONÍVEIS PARA O ATUAL EXERCÍCIO	IMPACTO DA PROPOSTA/INICIATIVA 81						
		Ano N	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)		
Artigo …….								

Relativamente às receitas afetadas, especificar a(s) rubrica(s) orçamental(ais) de despesas envolvida(s).

Outras observações (p. ex., método/fórmula utilizado/a para o cálculo do impacto sobre as receitas ou qualquer outra informação).

(1) https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pt.pdf .
(2) Comissão Europeia: Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança [COM(2020) 65 final].
(3) Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020, p. 6].
(4) Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].
(5) Conselho Europeu, Reunião do Conselho Europeu (19 de outubro de 2017) — Conclusões [EUCO 14/17, 2017, p. 8].
(6) Conselho da União Europeia, Inteligência artificial: b) Conclusões sobre o plano coordenado para a inteligência artificial — Adoção [6177/19, 2019].
(7) Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020].
(8) Conselho da União Europeia, Conclusões da Presidência — A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital [11481/20, 2020].
(9) Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].
(10) Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre o regime de responsabilidade civil aplicável à inteligência artificial [2020/2014(INL)].
(11) Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial [2020/2015(INI)].
(12) Projeto de relatório do Parlamento Europeu sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais [2020/2016(INI)].
(13) Projeto de relatório do Parlamento Europeu sobre a inteligência artificial na educação, na cultura e no setor audiovisual [2020/2017(INI)]. A Comissão adotou, neste contexto, o «Plano de Ação para a Educação Digital 2021-2027 — Reconfigurar a educação e a formação para a era digital» [COM(2020) 624 final], que prevê o desenvolvimento de orientações éticas em matéria de inteligência artificial e utilização de dados no ensino.
(14) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).
(15) Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).
(16) Ver a proposta de regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Diretiva 2000/31/CE [COM(2020) 825 final].
(17) Comunicação da Comissão: Construir o futuro digital da Europa [COM(2020) 67 final].
(18) Orientações para a Digitalização até 2030: a via europeia para a Década Digital .
(19) Proposta de regulamento relativo à governação de dados (Regulamento Governação de Dados) [COM(2020) 767].
(20) Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público [PE/28/2019/REV/1] (JO L 172 de 26.6.2019, p. 56).
(21) Comunicação da Comissão: Uma estratégia europeia para os dados [COM(2020) 66 final].
(22) Consultar todos os resultados da consulta aqui.
(23) Comissão Europeia: Aumentar a confiança numa inteligência artificial centrada no ser humano [COM(2019) 168].
(24) GPAN, Orientações éticas para uma IA de confiança , 2019.
(25) GPAN, Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment , 2020 [não traduzida para português].
(26) A Aliança da IA é um fórum multilateral lançado em junho de 2018, https://ec.europa.eu/digital-single-market/en/european-ai-alliance .

(27) Comissão Europeia: Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence [não traduzida para português].
(28) Para obter mais informações sobre todas as consultas realizadas, consultar o anexo 2 da avaliação de impacto.
(29) Grupo de Peritos de Alto Nível em Inteligência Artificial, Orientações éticas para uma IA de confiança , 2019.
(30) Também foram apoiados na Comunicação da Comissão «Aumentar a confiança numa inteligência artificial centrada no ser humano», de 2019.
(31) JO C […] de […], p. […].
(32) JO C […] de […], p. […].
(33) Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020, p. 6].
(34) Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].
(35) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).
(36) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).
(37) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (Diretiva sobre a Proteção de Dados na Aplicação da Lei) (*JO L 119 de 4.5.2016, p. 89).*
(38) Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).
(39) Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).
(40) Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação e fiscalização do mercado de tratores agrícolas e florestais (JO L 60 de 2.3.2013, p. 1).
(41) Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52).
(42) Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146).
(43) Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa à interoperabilidade do sistema ferroviário na União Europeia (JO L 138 de 26.5.2016, p. 44).
(44) Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1).
(45) Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento

Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1).
(46) Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1).
(47) Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1).
(48) Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico in vitro e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).
(49) Diretiva 2013/32/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional (JO L 180 de 29.6.2013, p. 60).
(50) Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (Código de Vistos) (JO L 243 de 15.9.2009, p. 1).
(51) Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).
(52) Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE (JO L 218 de 13.8.2008, p. 82).
(53) Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos e que altera a Diretiva 2004/42/CE e os Regulamentos (CE) n.º 765/2008 e (UE) n.º 305/2011 (Texto relevante para efeitos do EEE) (JO L 169 de 25.6.2019, p. 1).
(54) Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).
(55) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).
(56) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).
(57) Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (JO L 11 de 15.1.2002, p. 4).
(58) JO L 123 de 12.5.2016, p. 1.
(59) Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo

pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).
(60) Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).
(61) Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).
(62) Decisão-quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).
(63) Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 1).
(64) A que se refere o artigo 54.º, n.º 2, alíneas a) ou b), do Regulamento Financeiro.
(65) As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html .
(66) DD = dotações diferenciadas/DND = dotações não diferenciadas.
(67) EFTA: Associação Europeia de Comércio Livre.
(68) Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.
(69) Indicativo e dependente da disponibilidade orçamental.
(70) De acordo com a nomenclatura orçamental oficial.
(71) Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.
(72) Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.
(73) Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.
(74) Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…».
(75) Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.
(76) Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.
(77) Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.
(78) AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.
(79) Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).
(80) O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.
(81) No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.

COMISSÃO EUROPEIA

Bruxelas, 21.4.2021
COM(2021) 206 final

ANEXOS
da
Proposta de Regulamento do Parlamento Europeu e do Conselho
QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

ANEXO I

TÉCNICAS E ABORDAGENS NO DOMÍNIO DA INTELIGÊNCIA ARTIFICIAL referidas no artigo 3.º, ponto 1

a) Abordagens de aprendizagem automática, incluindo aprendizagem supervisionada, não supervisionada e por reforço, utilizando uma grande variedade de métodos, designadamente aprendizagem profunda;
b) Abordagens baseadas na lógica e no conhecimento, nomeadamente representação do conhecimento, programação (lógica) indutiva, bases de conhecimento, motores de inferência e de dedução, sistemas de raciocínio (simbólico) e sistemas periciais;
c) Abordagens estatísticas, estimação de Bayes, métodos de pesquisa e otimização.

ANEXO II

LISTA DA LEGISLAÇÃO DE HARMONIZAÇÃO DA UNIÃO
Secção A — Lista da legislação de harmonização da União baseada no novo quadro legislativo

1.Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa às máquinas e que altera a Diretiva 95/16/CE (JO L 157 de 9.6.2006, p. 24) [revogada pelo Regulamento Máquinas];

2.Diretiva 2009/48/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009, relativa à segurança dos brinquedos (JO L 170 de 30.6.2009, p. 1);
3.Diretiva 2013/53/UE do Parlamento Europeu e do Conselho, de 20 de novembro de 2013, relativa às embarcações de recreio e às motas de água e que revoga a Diretiva 94/25/CE (JO L 354 de 28.12.2013, p. 90);
4.Diretiva 2014/33/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante a ascensores e componentes de segurança para ascensores (JO L 96 de 29.3.2014, p. 251);
5.Diretiva 2014/34/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros relativa a aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas (JO L 96 de 29.3.2014, p. 309);
6.Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62);
7.Diretiva 2014/68/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos sob pressão no mercado (JO L 189 de 27.6.2014, p. 164);
8.Regulamento (UE) 2016/424 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo às instalações por cabo e que revoga a Diretiva 2000/9/CE (JO L 81 de 31.3.2016, p. 1);
9.Regulamento (UE) 2016/425 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos equipamentos de proteção individual e que revoga a Diretiva 89/686/CEE do Conselho (JO L 81 de 31.3.2016, p. 51);
10.Regulamento (UE) 2016/426 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos aparelhos a gás e que revoga a Diretiva 2009/142/CE do Conselho (JO L 81 de 31.3.2016, p. 99);
11.Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1);
12.Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico in vitro e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).

Secção B — Lista de outra legislação de harmonização da União

1.Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).
2.Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52);
3.Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação e fiscalização do mercado de tratores agrícolas e florestais (JO L 60 de 2.3.2013, p. 1);

4.Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146);
5.Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa à interoperabilidade do sistema ferroviário na União Europeia (JO L 138 de 26.5.2016, p. 44).
6.Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1); 3. Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) n.º 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1);
7.Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1), no que se refere ao projeto, fabrico e colocação no mercado de aeronaves a que se refere o artigo 2.º, n.º 1, alíneas a) e b), na parte relativa a aeronaves não tripuladas e aos seus motores, hélices, peças e equipamento de controlo remoto.

ANEXO III

SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO A QUE SE REFERE O ARTIGO 6.º, N.º 2

Os sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2, são os sistemas de IA incluídos num dos domínios a seguir enumerados:
1.Identificação biométrica e categorização de pessoas singulares:
a) Sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância «em tempo real» e «em diferido» de pessoas singulares;
2.Gestão e funcionamento de infraestruturas críticas:
a) Sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo do trânsito rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade.
3.Educação e formação profissional:
a) Sistemas de IA concebidos para serem utilizados para fins de determinação do acesso ou da afetação de pessoas singulares a instituições de ensino e de formação profissional;

b) Sistemas de IA concebidos para serem utilizados para fins de avaliação de estudantes em instituições de ensino ou de formação profissional e de avaliação de participantes nos testes habitualmente exigidos para admissão em instituições de ensino.
4.Emprego, gestão de trabalhadores e acesso ao emprego por conta própria:
a) Sistemas de IA concebidos para serem utilizados no recrutamento ou na seleção de pessoas singulares, designadamente para divulgação de vagas, aplicações de triagem ou filtragem, avaliação de candidatos no decurso de entrevistas ou testes;
b) Sistemas de IA concebidos para serem utilizados na tomada de decisões sobre promoções ou cessações de relações contratuais de trabalho, na repartição de tarefas e no controlo e avaliação do desempenho e do comportamento de pessoas envolvidas nas referidas relações.
5.Acesso a serviços privados e a serviços e prestações públicas essenciais, bem como o usufruto dos mesmos:
a) Sistemas de IA concebidos para serem utilizados por autoridades públicas ou em nome de autoridades públicas para avaliar a elegibilidade de pessoas singulares quanto a prestações e serviços públicos de assistência, bem como para conceder, reduzir, revogar ou recuperar tais prestações e serviços;
b) Sistemas de IA concebidos para serem utilizados para avaliar a capacidade de endividamento de pessoas singulares ou estabelecer a sua classificação de crédito, com exceção dos sistemas de IA colocados em serviço por fornecedores de pequena dimensão para utilização própria;
c) Sistemas de IA concebidos para serem utilizados no envio ou no estabelecimento de prioridades no envio de serviços de resposta a emergências, incluindo bombeiros e assistência médica.
6.Manutenção da ordem pública:
a) Sistemas de IA concebidos para serem utilizados por autoridades policiais em avaliações individuais de riscos relativamente a pessoas singulares, a fim de determinar o risco de uma pessoa singular cometer infrações ou voltar a cometer infrações ou o risco para potenciais vítimas de infrações penais;
b) Sistemas de IA concebidos para serem utilizados por autoridades policiais como polígrafos e instrumentos similares ou para detetar o estado emocional de uma pessoa singular;
c)Sistemas de IA concebidos para serem utilizados por autoridades policiais para detetar falsificações profundas referidas no artigo 52.º, n.º 3;
d)Sistemas de IA concebidos para serem utilizados por autoridades policiais para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou repressão de infrações penais;
e) Sistemas de IA concebidos para serem utilizados por autoridades policiais para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis de pessoas singulares, na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos;
f) Sistemas de IA concebidos para serem utilizados por autoridades policiais para definir o perfil de pessoas singulares, na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, no decurso da deteção, investigação ou repressão de infrações penais;
g) Sistemas de IA concebidos para serem utilizados no estudo analítico de crimes relativos a pessoas singulares, permitindo às autoridades policiais pesquisar grandes conjuntos de dados complexos, relacionados ou não relacionados, disponíveis em diferentes fontes de dados ou em diferentes formatos de dados, no intuito de identificar padrões desconhecidos ou descobrir relações escondidas nos dados.

7.Gestão da migração, do asilo e do controlo das fronteiras:
a) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes como polígrafos e instrumentos similares ou para detetar o estado emocional de uma pessoa singular;
b) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes para avaliar riscos, incluindo um risco para a segurança, um risco de imigração irregular ou um risco para a saúde, representados por uma pessoa singular que pretenda entrar ou tenha entrado no território de um Estado-Membro;
c) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes para verificar a autenticidade de documentos de viagem e documentos comprovativos de pessoas singulares e detetar documentos não autênticos por meio da verificação dos seus elementos de segurança;
d) Sistemas de IA concebidos para auxiliar autoridades públicas competentes na análise dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, no que toca à elegibilidade das pessoas singulares que requerem determinado estatuto.
8.Administração da justiça e processos democráticos:
a) Sistemas de IA concebidos para auxiliar uma autoridade judiciária na investigação e na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos.

ANEXO IV

DOCUMENTAÇÃO TÉCNICA referida no artigo 11.º, n.º 1

A documentação técnica referida no artigo 11.º, n.º 1, deve conter, pelo menos, as informações indicadas a seguir, consoante aplicável ao sistema de IA em causa:

1.Uma descrição geral do sistema de IA, nomeadamente:

a)A finalidade prevista, a(s) pessoa(s) responsáveis pelo seu desenvolvimento, a data e a versão do sistema;

b)De que forma o sistema de IA interage ou pode ser utilizado para interagir com hardware ou software que não faça parte do próprio sistema de IA, se for caso disso;

c)As versões do software ou firmware instalado e quaisquer requisitos relacionados com a atualização das versões;

d)A descrição de todas as formas sob as quais o sistema de IA é colocado no mercado ou colocado em serviço;

e)A descrição do hardware no qual se pretende executar o sistema de IA;

f)Se o sistema de IA for um componente de produtos, fotografias ou ilustrações que revelem as características externas, a marcação e a disposição interna desses produtos;

g)Instruções de utilização para o utilizador e, se for caso disso, instruções de instalação;

2.Uma descrição pormenorizada dos elementos do sistema de IA e do respetivo processo de desenvolvimento, incluindo:

a)Os métodos utilizados e os passos dados com vista ao desenvolvimento do sistema de IA, incluindo, se for caso disso, o recurso a sistemas ou ferramentas previamente treinados fornecidos por terceiros e de que forma estes foram utilizados, integrados ou modificados pelo fornecedor;

b)As especificações de conceção do sistema, designadamente a lógica geral do sistema de IA e dos algoritmos; as principais opções de conceção, nomeadamente a lógica subjacente e os pressupostos utilizados, também

no respeitante às pessoas ou grupos de pessoas em relação às quais se pretende que o sistema seja utilizado; as principais opções de classificação; o que se pretende otimizar com o sistema e a importância dos diferentes parâmetros; as decisões acerca de eventuais cedências em relação às soluções técnicas adotadas para cumprir os requisitos definidos no título III, capitulo 2;

c)A descrição da arquitetura do sistema, explicando de que forma os componentes de software se incorporam ou enriquecem mutuamente e como se integram no processamento global; os recursos computacionais utilizados para desenvolver, treinar, testar e validar o sistema de IA;

d)Se for caso disso, os requisitos de dados em termos de folhas de dados que descrevam as metodologias e técnicas de treino e os conjuntos de dados de treino utilizados, incluindo informações sobre a proveniência desses conjuntos de dados, o seu âmbito e as suas principais características; de que forma os dados foram obtidos e selecionados; procedimentos de rotulagem (por exemplo, para aprendizagem supervisionada), metodologias de limpeza de dados (por exemplo, deteção de valores atípicos);

e)Análise das medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo uma análise das soluções técnicas necessárias para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores, em conformidade com o artigo 13.º, n.º 3, alínea d);

f)Se for caso disso, uma descrição pormenorizada das alterações predeterminadas do sistema de IA e do seu desempenho, juntamente com todas as informações pertinentes relacionadas com as soluções técnicas adotadas para assegurar a conformidade contínua do sistema de IA com os requisitos aplicáveis estabelecidos no título III, capítulo 2;

g)Os procedimentos de validação e teste aplicados, incluindo informações sobre os dados de validação e teste utilizados e as principais características desses dados; as métricas utilizadas para aferir a exatidão, a solidez, a cibersegurança e a conformidade com outros requisitos aplicáveis estabelecidos no título III, capítulo 2, bem como potenciais impactos discriminatórios; registos dos testes e todos os relatórios de teste datados e assinados pelas pessoas responsáveis, incluindo no respeitante às alterações predeterminadas referidas na alínea f).

3.Informações pormenorizadas sobre o acompanhamento, o funcionamento e o controlo do sistema de IA, especialmente no que diz respeito: às suas capacidades e limitações de desempenho, incluindo os níveis de exatidão no tocante a pessoas ou grupos de pessoas específicos em relação às quais se pretende que o sistema seja utilizado e o nível geral esperado de exatidão em relação à finalidade prevista; os resultados não pretendidos mas previsíveis e as fontes de riscos para a saúde e a segurança, os direitos fundamentais e a proteção contra a discriminação atendendo à finalidade prevista do sistema de IA; as medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores; especificações relativas aos dados de entrada, consoante apropriado;

4.Uma descrição pormenorizada do sistema de gestão de riscos em conformidade com o artigo 9.º;

5.A descrição de todas as alterações introduzidas no sistema ao longo do seu ciclo de vida;
6.Uma lista de normas harmonizadas aplicadas total ou parcialmente, cujas referências tenham sido publicadas no Jornal Oficial da União Europeia; caso não tenham sido aplicadas tais normas harmonizadas, uma descrição pormenorizada das soluções adotadas para cumprir os requisitos estabelecidos no título III, capítulo 2, incluindo uma lista de outras normas pertinentes e especificações técnicas aplicadas;
7.Uma cópia da declaração de conformidade UE;
8.Uma descrição pormenorizada do sistema existente para avaliar o desempenho do sistema de IA na fase de pós-comercialização em conformidade com o artigo 61.º, nomeadamente o plano de acompanhamento pós-comercialização referido no artigo 61.º, n.º 3.

ANEXO V
DECLARAÇÃO DE CONFORMIDADE UE

A declaração de conformidade UE referida no artigo 48.º deve conter todas as seguintes informações:

1.Nome e tipo do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;
2.Nome e endereço do fornecedor ou, se aplicável, do mandatário;
3.Menção de que a declaração de conformidade UE é emitida sob a exclusiva responsabilidade do fornecedor;
4.Menção que ateste que o sistema de IA em causa é conforme com o presente regulamento e, se for caso disso, com outra legislação da União aplicável que preveja a emissão de declarações de conformidade UE;
5.Referências a quaisquer normas harmonizadas aplicáveis utilizadas ou a quaisquer outras especificações comuns em relação às quais é declarada a conformidade;
6.Se for caso disso, nome e número de identificação do organismo notificado, descrição do procedimento de avaliação da conformidade adotado e identificação do certificado emitido;
7.Local e data de emissão da declaração, nome e cargo da pessoa que assina, bem como indicação da pessoa em nome de quem assina, assinatura.

ANEXO VI
PROCEDIMENTO DE AVALIAÇÃO DA CONFORMIDADE BASEADO NO CONTROLO INTERNO

1.O procedimento de avaliação da conformidade baseado no controlo interno é o descrito nos pontos 2 a 4.

2.O fornecedor verifica se o sistema de gestão da qualidade aplicado se encontra em conformidade com os requisitos do artigo 17.º.

3.O fornecedor analisa as informações contidas na documentação técnica para determinar a conformidade do sistema de IA com os requisitos essenciais aplicáveis estabelecidos no título III, capítulo 2.

4.O fornecedor também verifica se o processo de conceção e desenvolvimento do sistema de IA e do seu acompanhamento pós-comercialização referido no artigo 61.º estão de acordo com a documentação técnica.

ANEXO VII

CONFORMIDADE BASEADA NA AVALIAÇÃO DO SISTEMA DE GESTÃO DA QUALIDADE E NA AVALIAÇÃO DA DOCUMENTAÇÃO TÉCNICA

1.Introdução

A conformidade baseada na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica é o procedimento de avaliação da conformidade descrito nos pontos 2 a 5.

2.Visão geral

O sistema de gestão da qualidade aprovado para efeitos de conceção, desenvolvimento e testagem de sistemas de IA nos termos do artigo 17.º é analisado em conformidade com o ponto 3 e está sujeito à fiscalização especificada no ponto 5. A documentação técnica do sistema de IA é analisada em conformidade com o ponto 4.

3.Sistema de gestão da qualidade

3.1.O pedido do fornecedor inclui:

a)O nome e o endereço do fornecedor e, se for apresentado pelo mandatário, o nome e o endereço deste último;

b)A lista dos sistemas de IA abrangidos pelo mesmo sistema de gestão da qualidade;

c)A documentação técnica de cada sistema de IA abrangido pelo mesmo sistema de gestão da qualidade;

d)A documentação relativa ao sistema de gestão da qualidade, que abrange todos os aspetos enunciados no artigo 17.º;

e)Uma descrição dos procedimentos em vigor para assegurar a adequação e eficácia do sistema de gestão da qualidade;

f)Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2.O sistema de gestão da qualidade é avaliado pelo organismo notificado, que determina se esse sistema cumpre os requisitos referidos no artigo 17.º.

A decisão é notificada ao fornecedor ou ao seu mandatário.

A notificação inclui as conclusões da avaliação do sistema de gestão da qualidade e a decisão de avaliação fundamentada.

3.3.O fornecedor deve continuar a aplicar e a manter o sistema de gestão da qualidade aprovado de maneira que este permaneça adequado e eficiente.

3.4.O fornecedor deve comunicar ao organismo notificado qualquer alteração planeada do sistema de gestão da qualidade aprovado ou da lista de sistemas de IA abrangidos por este último.

As alterações propostas são analisadas pelo organismo notificado, a quem cabe decidir se o sistema de gestão da qualidade alterado continua a satisfazer os

requisitos enunciados no ponto 3.2 ou se será necessário proceder a nova avaliação.

O organismo notificado notifica o fornecedor da sua decisão. A notificação inclui as conclusões da análise das alterações e a decisão de avaliação fundamentada.

4.Controlo da documentação técnica.

4.1.Além do pedido referido no ponto 3, o fornecedor deve apresentar junto do organismo notificado da sua escolha um pedido de avaliação da documentação técnica relativa ao sistema de IA que o fornecedor tenciona colocar no mercado ou colocar em serviço e que seja abrangido pelo sistema de gestão da qualidade referido no ponto 3.

4.2.O pedido deve incluir:

a)O nome e o endereço do fornecedor;

b)Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado;

c)A documentação técnica referida no anexo IV.

4.3.O organismo notificado analisa a documentação técnica. Para o efeito, o organismo notificado deve dispor de total acesso aos conjuntos de dados de treino e teste utilizados pelo fornecedor, incluindo através de interfaces de programação de aplicações ou outros meios e ferramentas adequadas que possibilitem o acesso remoto.

4.4.Ao analisar a documentação técnica, o organismo notificado pode requerer que o fornecedor apresente mais provas ou realize mais testes de maneira que permita uma adequada avaliação da conformidade do sistema de IA com os requisitos estabelecidos no título III, capítulo 2. Se o organismo notificado não ficar satisfeito com os testes realizados pelo fornecedor, deve realizar diretamente os testes adequados que sejam necessários.

4.5.Sempre que necessário para avaliar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no título III, capítulo 2, e mediante pedido fundamentado, deve também ser concedido ao organismo notificado o acesso ao código-fonte do sistema de IA.

4.6.A decisão é notificada ao fornecedor ou ao seu mandatário. A notificação inclui as conclusões da avaliação da documentação técnica e a decisão de avaliação fundamentada.

Se o sistema de IA estiver em conformidade com os requisitos estabelecidos no título III, capítulo 2, o organismo notificado emite um certificado UE de avaliação da documentação técnica. Esse certificado deve indicar o nome e o endereço do fornecedor, as conclusões do exame, as (eventuais) condições da sua validade e os dados necessários à identificação do sistema de IA.

O certificado e os seus anexos devem conter todas as informações necessárias para permitir a avaliação da conformidade do sistema de IA e o controlo do sistema de IA durante a utilização, se for caso disso.

Se o sistema de IA não estiver em conformidade com os requisitos estabelecidos no título III, capítulo 2, o organismo notificado recusa a emissão de um certificado UE de avaliação da documentação técnica e informa o requerente do facto, fundamentando pormenorizadamente as razões da sua recusa.

Se o sistema de IA não cumprir o requisito relativo aos dados utilizados para o treinar, será necessário voltar a treinar o sistema de IA antes da apresentação do pedido de nova avaliação da conformidade. Nesse caso, a decisão de avaliação fundamentada pela qual o organismo notificado recusa a emissão do certificado UE de avaliação da documentação técnica inclui considerações específicas sobre a qualidade dos dados utilizados para treinar o sistema de IA, designadamente as razões da não conformidade.

4.7.Qualquer alteração do sistema de IA que possa afetar a conformidade do sistema de IA com os requisitos ou com a finalidade prevista deve ser aprovada pelo organismo notificado que emitiu o certificado UE de avaliação da documentação técnica. O fornecedor informa o referido organismo notificado se tencionar introduzir alterações como as supramencionadas ou se, de algum outro modo, tiver conhecimento da ocorrência dessas alterações. As alterações planeadas são examinadas pelo organismo notificado, a quem cabe decidir se estas exigem que se proceda a uma nova avaliação da conformidade nos termos do artigo 43.º, n.º 4, ou se a situação pode ser resolvida com um aditamento ao certificado UE de avaliação da documentação técnica. Neste último caso, o organismo notificado examina as alterações, notifica o fornecedor da sua decisão e, se as alterações forem aprovadas, emite ao fornecedor um aditamento ao certificado UE de avaliação da documentação técnica.

5.Fiscalização do sistema de gestão da qualidade aprovado.

5.1.O objetivo da fiscalização realizada pelo organismo notificado a que se refere o ponto 3 é garantir que o fornecedor cumpre fielmente os termos e as condições do sistema de gestão da qualidade aprovado.

5.2.Para efeitos de avaliação, o fornecedor deve autorizar o organismo notificado a aceder às instalações onde decorre a conceção, o desenvolvimento e a testagem dos sistemas de IA. O fornecedor deve igualmente partilhar com o organismo notificado todas as informações necessárias.

5.3.O organismo notificado efetua auditorias periódicas para se certificar de que o fornecedor mantém e aplica o sistema de gestão da qualidade e faculta ao fornecedor um relatório de auditoria. No contexto das referidas auditorias, o organismo notificado pode realizar testes adicionais aos sistemas de IA em

relação aos quais foi emitido um certificado UE de avaliação da documentação técnica.

ANEXO VIII

INFORMAÇÕES A APRESENTAR AQUANDO DO REGISTO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO NOS TERMOS DO ARTIGO 51.º

As informações a seguir indicadas devem ser fornecidas e, subsequentemente, mantidas atualizadas no respeitante a sistemas de IA de risco elevado a registar em conformidade com o artigo 51.º.

1.Nome, endereço e contactos do fornecedor;

2.Se as informações forem apresentadas por outra pessoa em nome do fornecedor, nome, endereço e contactos dessa pessoa;

3.Nome, endereço e contactos do mandatário, se for caso disso;

4.Designação comercial do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

5.Descrição da finalidade prevista do sistema de IA;

6.Estado do sistema de IA (no mercado ou em serviço; já não se encontra no mercado/em serviço; retirado);

7.Tipo, número e data de validade do certificado emitido pelo organismo notificado e o nome ou número de identificação desse organismo notificado, quando aplicável;

8.Uma cópia digitalizada do certificado referido no ponto 7, quando aplicável;

9.Os Estados-Membros onde o sistema de IA está ou foi colocado no mercado ou colocado em serviço ou disponibilizado na União;

10.Uma cópia da declaração de conformidade UE referida no artigo 48.º;

11.Instruções de utilização em formato eletrónico; esta informação não é fornecida no que respeita a sistemas de IA de risco elevado nos domínios da manutenção da ordem pública e da gestão da migração, do asilo e do controlo das fronteiras, referidos no anexo III, pontos 1, 6 e 7;

12.URL para informações adicionais (opcional).

ANEXO IX

Legislação da União relativa a sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça

1.Sistema de Informação de Schengen

a)Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular (JO L 312 de 7.12.2018, p. 1).

b)Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

c)Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

2.Sistema de Informação sobre Vistos

a)Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que altera o Regulamento (CE) n.º 767/2008, o Regulamento (CE) n.º 810/2009, o Regulamento (UE) 2017/2226, o Regulamento (UE) 2016/399, o Regulamento XX/2018 [Regulamento Interoperabilidade] e a Decisão 2004/512/CE e que revoga a Decisão 2008/633/JAI do Conselho [COM(2018) 302 final]. A atualizar assim que os colegisladores adotarem o regulamento (abril/maio de 2021).

3.Eurodac

a)Proposta alterada de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo à criação do sistema «Eurodac» de comparação de dados biométricos para efeitos da aplicação efetiva do Regulamento (UE) XXX/XXX [Regulamento Gestão do Asilo e da Migração] e do Regulamento (UE) XXX/XXX [Regulamento Reinstalação], da identificação de nacionais de países terceiros ou apátridas em situação irregular, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera os Regulamentos (UE) 2018/1240 e (UE) 2019/818 [COM(2020) 614 final].

4.Sistema de Entrada/Saída

a)Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção

de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (JO L 327 de 9.12.2017, p. 20).

5.Sistema Europeu de Informação e Autorização de Viagem

a)Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (JO L 236 de 19.9.2018, p. 1).

b)Regulamento (UE) 2018/1241 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que altera o Regulamento (UE) 2016/794 para efeitos da criação de um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) (JO L 236 de 19.9.2018, p. 72).

6.Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros e de apátridas

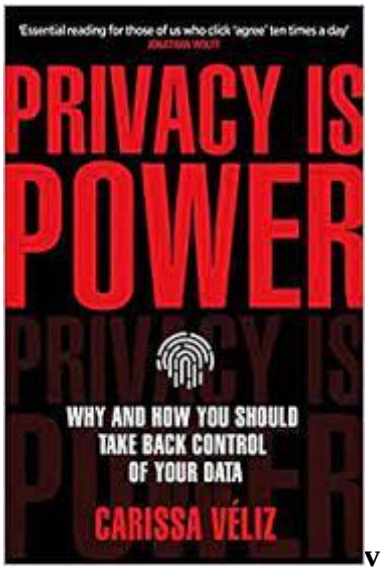
a)Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726 (JO L 135 de 22.5.2019, p. 1).

7.Interoperabilidade

a)Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos (JO L 135 de 22.5.2019, p. 27).

b)Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração (JO L 135 de 22.5.2019, p. 85).

IV_Recensões



Privacy is Power

Carissa Vélez
Penguin Random House, UK, 2020

Alexandre Sousa Pinheiro[1]

Trata-se de um trabalho interessante, de tipo "enquadrador" ao tema da privacidade.

Rigorosamente tem a natureza de um "texto de denúncia", alertando para os perigos que afetam a privacidade no mundo da Internet, tornando o sujeito passível de uma vigilância constante. A autora faz vingar, igualmente, uma componente de contestação política sobre a "data economy" ao longo do livro.

Encontramos aqui as maiores virtudes e, ao mesmo tempo, debilidades da obra: uma crítica completa e desenvolvida aos ataques à *privacy* mas, amiúde, desacompanhada de construções sistemáticas limitando-se a dar voz pública às premonições negativas sobre a evolução do tratamento da informação pessoal no mundo da Internet e da inteligência artificial.

Dividido em seis capítulos, o primeiro relativo aos "abutres dos dados" compõe-se por parágrafos, cada um relacionado com recolha ou utilização indevida de informação pessoal. A entidade heresiarca é o Facebook, e as curtas narrativas baseiam-se em situações que agitam neófitos nas áreas da privacidade e da proteção de dados, mas não fornecem elementos novos a quem trabalhe na área ou leia habitualmente sobre o tema.

O capítulo II – "How did we get here" – apela ao 11 de setembro de 2001 e aos desenvolvimentos de controlo coletivo desenvolvidos desde aí, com a influência evidente e reconhecida de Shoshana Zuboff (p. 29). Vélez, após descrever a evolução da Google de companhia publicitária até importante instância de poder, adverte para a perda do controlo de padrões de privacidade durante a pandemia em curso (p. 45).

Em uma lúcida observação a autora refere que a a recolha maciça de dados é tóxica, mas desenvolvida através de *slow-acting poison* (p. 43). Com base neste pensamento introduz

o capítulo III – "Privacy is Power" – onde se desenvolvem temas já tratados e narrativas habitualmente conhecidas na comunidade de proteção de dados (enfaticamente, os perigos do pensamento infantil de que "quem não deve não teme" (p. 48). Vélez apresenta a informação recolhida como poder que afeta o titular, particularmente quando está na titularidade das grandes empresas tecnológicas com amplos poderes para condicionar a liberdade pessoal, dando espaço significativo ao modelo chinês.

As "poisoned societies", refere a autora, colocam em crise a segurança nacional, corrompem a democracia, afetam os valores liberais através duma cultura de vigilância e afetam a segurança das pessoas (p. 97), concluindo que as previsões sombrias do futuro assentam nos acontecimentos do passado (*maxime* recurso a registos para identificar judeus na Alemanha nazi ou os comportamentos adotados na RDA pela STASI) (p. 114).

O capítulo V – "Pulling the Plug" – expressa o que a autora considera necessário para desmantelar a economia baseada na vigilância digital: terminar com publicidade personalizada (pp. 119 e ss); terminar com o negácio de dados pessoais (pp. 126 e ss); terminar com a recolha de dados por defeito (pp. 130 e ss); terminar com as intervenções digitais subreptícias (pp. 134 e ss), diminuir a vigilância governamental (pp. 152 e ss); proibir equipamento de vigilância (p. 154) e proteger as crianças (pp. 155 e ss).

No capítulo VI – "What you can do ?" – vertem-se boas praticas para as relações que envolvam dados pessoais.

Numa interessante conclusão, Carissa Vélez afirma *Privacy is how we blind the system so that it treats us impartially and fairly* (p. 208).

"Privacy is Power" traduz-se num trabalho honesto de introdução aos perigos que a privacidade pode sofrer num mundo digital.

Quem pretenda leituras duras e profundas, que opte por autores mais sólidos, à cabeça por Shoshana Zuboff.

Direito e Inteligência Artificial – em Defesa do Humano

Juarez Freitas e Thimas Bellini Freitas
Editora Fórum, Belo Horizonte, 2020

Márcia Santana Fernandes[1]

A obra *Direito e Inteligência Artificial – em Defesa do Humano,* de autoria de Juarez Freitas e Thomas Bellini Freitas, publicado pela Editora Fórum, Belo Horizonte, em 2020 aborda tema relevante e disruptivo nos estudos de interface da tecnologia e do Direito.

A Inteligência Artificial (IA) impõe uma avaliação dos riscos e oportunidades associados à sua incorporação na vida e no viver dos seres humanos. Luciano Floridi[311], autor relevante nesta temática, referido também pelos autores, destaca a importância de refletir, pesquisar e compreender, em sentido amplo, os impactos da AI na vida dos seres humanos, individual ou coletivamente. É necessário compreender o ambiente da informação e sua transformação, conhecer o que Floridi denominou *Infosfera* (*Infosphere*, neologismo a partir de biosfera), pois a informação está presente no mundo vivo e em tudo que corresponde ao humano. E para compreender a natureza intrínseca da informação e sua transformação, também é necessária uma *reontologia* (*re-ontology)*, isto é uma forma radical de reengenharia; que transforma a natureza intrínseca, sua ontologia, ou seja, o próprio ser.[312]

Os diferentes tipos de IA apresentam múltiplos desafios éticos, legais e sociais. Os sistemas de IA envolvidos com processos de percepção foram incorporados com as

[311] FLORIDI, Luciano. Group privacy: a defence and an interpretation. In: FLORIDI, Luciano TAYLOR, Linnet; VAN DER SLOOT, Bart (Eds.). *Group privacy:* new challenges of data technologies. New York: Springer International Publishing, 2017, pp. 83-100; FLORIDI, Luciano. *The ethics of information*. Oxford: Oxford University Press, 2013.

[312] FERNANDES, Márcia S. Privacidade, sociedade da informação e Big Data In: Direito, Cultura e Método - Leituras da obra de Judith Martins-Costa. (Org.) BENETTI, G.; CORREA, A. R.; FERNANDES, M.S.; NITSCHKE, G. C. M.; PARGENDLER, M.; VARELA, L. B. 1ª Ed., Rio de Janeiro: GZ Editora, 2019, v.1, p. 182-210.

novas tecnologias de imagem e tratamento de sinais. Da mesma forma, os sistemas de IA na área de comunicação têm permitido realizar interações antes inexistentes e facilitar o acesso a dados e informações. A maior preocupação envolve as áreas de planejamento, conhecimento e raciocínio, pois os sistemas de IA se associam diretamente ao processo de tomada de decisão.[313]

Justamente, nas questões relacionadas à *regulação das decisões algorítmicas* é que reside o núcleo duro da obra de Juarez Freitas e Thomas Freitas. Os autores nos nove capítulos, em que a obra está organizada, abordam desde aspectos conceituais centrais, possíveis impactos e vieses, aos impactos éticos e jurídicos, de decisões que têm como substrato os algoritmos.

Os autores claramente destacam, no Capítulo 7 da Obra, a *explicabilidade* que *é diretriz mandatória para a AI ética e respeitadora dos direitos humanos, de modo a fazer explícitos os fundamentos das decisões algorítmicas, impedindo que tais escolhas relativamente autônomas restem desacompanhadas da inteligível motivação.*[314]

Da mesma forma, os autores não limitam sua abordagem ao diagnóstico da situação nuclear da obra, mas sim apresentam em seu Capítulo 9, aspectos relacionados à responsabilidade civil e criminal, no que concerne a situações envolvidas na tomada de decisão algorítmica. Neste Capítulo derradeiro, tratam também de alguns efeitos na área da Propriedade Intelectual, com foco na faceta dos Direitos Autorais.

Por fim, merece destacar que a obra de Freitas e Freitas, cita e refere autores relevantes para o estudo da temática e de sua interface com o Direito e outras áreas relacionadas. A cuidadosa e seleta organização e escolha das referências, poderá auxiliar aqueles interessados em enveredar no estudo interdisciplinar, que envolve a interface entre as áreas de sistemas e tecnologia, Ética e o Direito.

[313] FERNANDES, Márcia S. e GOLDIM, José Roberto. Inteligência Artificial e Processo de Tomada de Decisão em Saúde: riscos e oportunidades, Capítulo em desenvolvimento para publicação internacional, em 2022.
[314] FREITAS, Juarez e FREITAS, Thomas Bellini. *Direito e Inteligência Artificial – em Defesa do Humano, 1ª Ed.*, Belo Horizonte: Editora Fórum, 2020, p.101.